

Security and Privacy of Electronic Healthcare Records

Concepts, paradigms and solutions

Edited by

Sudeep Tanwar, Sudhanshu Tyagi and Neeraj Kumar



THE IET BOOK SERIES ON E-HEALTH TECHNOLOGIES

Security and Privacy of Electronic Healthcare Records

IET Book Series on e-Health Technologies – Call for authors

Book Series Editor: Professor Joel P. C. Rodrigues, the National Institute of Telecommunications (Inatel), Brazil and Instituto de Telecomunicações, Portugal

While the demographic shifts in populations display significant socio-economic challenges, they trigger opportunities for innovations in e-Health, m-Health, precision and personalized medicine, robotics, sensing, the Internet of Things, cloud computing, Big Data, Software Defined Networks, and network function virtualization. Their integration is however associated with many technological, ethical, legal, social and security issues. This new Book Series aims to disseminate recent advances for e-Health Technologies to improve healthcare and people's wellbeing.

Topics considered include Intelligent e-Health systems, electronic health records, ICT-enabled personal health systems, mobile and cloud computing for eHealth, health monitoring, precision and personalized health, robotics for e-Health, security and privacy in e-Health, ambient-assisted living, telemedicine, Big Data, and IoT for e-Health and more.

Proposals for coherently integrated International multi-authored edited or co-authored handbooks and research monographs will be considered for this Book Series. Each proposal will be reviewed by the Book Series Editor with additional external reviews from independent reviewers. Please email your book proposal for the IET Book Series on e-Health Technologies to Professor Joel Rodrigues at joeljr@ieee.org or joeljr@inatel.br

Security and Privacy of Electronic Healthcare Records

Concepts, paradigms and solutions

Edited by

Sudeep Tanwar, Sudhanshu Tyagi and Neeraj Kumar

Published by The Institution of Engineering and Technology, London, United Kingdom

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no. 211014) and Scotland (no. SC038698).

© The Institution of Engineering and Technology 2020

First published 2019

This publication is copyright under the Berne Convention and the Universal Copyright Convention. All rights reserved. Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may be reproduced, stored or transmitted, in any form or by any means, only with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at the undermentioned address:

The Institution of Engineering and Technology
Michael Faraday House
Six Hills Way, Stevenage
Herts, SG1 2AY, United Kingdom

www.theiet.org

While the authors and publisher believe that the information and guidance given in this work are correct, all parties must rely upon their own skill and judgement when making use of them. Neither the authors nor publisher assumes any liability to anyone for any loss or damage caused by any error or omission in the work, whether such an error or omission is the result of negligence or any other cause. Any and all such liability is disclaimed.

The moral rights of the authors to be identified as authors of this work have been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

British Library Cataloguing in Publication Data

A catalogue record for this product is available from the British Library

ISBN 978-1-78561-898-7 (hardback)

ISBN 978-1-78561-899-4 (PDF)

Typeset in India by MPS Limited

Printed in the UK by CPI Group (UK) Ltd, Croydon

Contents

About the editors	xvii
Preface	xix
Part I Technological developments in healthcare	1
1 Introduction	3
<i>Sudeep Tanwar, Rajesh Gupta, Aparna Kumari, Sudhanshu Tyagi, and Neeraj Kumar</i>	
1.1 Personal health record	4
1.2 Privacy and security issue in PHR	5
1.2.1 Insider curiosity and subordination	5
1.2.2 Accidental disclosure	5
1.2.3 Outsider intrusion	5
1.2.4 Uncontrolled secondary usage	5
1.3 Electronic health record	6
1.3.1 Advantages of having EHRs	7
1.4 What are the benefits of EHR technology?	8
1.5 Security and privacy concern in EHR	8
1.5.1 Privacy in EHR	9
1.5.2 Security in EHR	11
1.6 Challenges in security and privacy	12
1.6.1 Verification of user	12
1.6.2 Integrity and confidentiality	12
1.6.3 Access control	12
1.6.4 Data control	12
1.6.5 Data security policies	12
1.6.6 Profiles of user	12
1.6.7 Misuse of health record	13
References	13
2 Introduction to healthcare information privacy and security concerns	17
<i>Anoop Kumar Pandey</i>	
2.1 Introduction to electronic health records	17
2.1.1 Paper-based records	18
2.1.2 Moving toward EHR	19
2.2 Components of an EHR	22
2.2.1 Core components of an EHR	22
2.2.2 Additional desirable capabilities	23

2.3	Challenges in EHR adoption	24
2.3.1	Technological makeover	24
2.3.2	Financial challenge	24
2.3.3	Personnel cooperation	25
2.3.4	Interoperability	25
2.3.5	Integration with other systems	25
2.3.6	Usability	25
2.3.7	Data completeness and correctness	26
2.3.8	Storage of EHR data	27
2.3.9	Security of EHR data	27
2.3.10	Privacy concerns	28
2.4	Security concerns in healthcare information	29
2.4.1	Physical security	29
2.4.2	Application security	29
2.4.3	Server security	30
2.4.4	Periphery security	30
2.4.5	Storage and communication security	30
2.4.6	Ubiquitous device security	30
2.4.7	Preserving confidentiality	31
2.4.8	Data integrity	31
2.4.9	Data availability	31
2.4.10	Audit trail	32
2.4.11	Mock drills	32
2.4.12	Data breach and mandatory disclosure	32
2.5	Curbing security concerns	33
2.6	Privacy concerns in healthcare information	34
2.6.1	Major issues driving privacy front	34
2.6.2	Privacy laws and guidelines	36
2.6.3	Using blockchain for privacy protection	38
2.6.4	Protecting patient data privacy	39
	References	39

3 Fundamentals of health-care system and general rules for security and privacy **43**

Hiral Patel, Meghna Patel, and Satyen Parikh

3.1	Introduction	43
3.1.1	What is EHR (electronic health record)?	43
3.1.2	Workflow of traditional medical care system	44
3.1.3	Workflow of electronic health record system	45
3.1.4	Advantages of the EHR system	47
3.2	Scratch for privacy and security concern	48
3.2.1	Background of health information privacy and security	48
3.2.2	Privacy and confidentiality	48
3.2.3	Security	49
3.2.4	Problems arise in security and privacy	49

3.3	The HIPAA rules and patient's rights for health care	50
3.3.1	The HIPAA privacy rule	51
3.3.2	The HIPAA security rule	52
3.3.3	The breach notification rule	52
3.4	Hazard capacity method for breaches	53
3.4.1	Revealing breaches	53
3.4.2	Examination and enforcement of potential ACT violations	53
3.4.3	Understanding patients' health information rights	54
3.5	Generalize E-health-care models	55
3.6	Conclusions and current scope of research	56
	References	56
4	Identity and access management systems	61
	<i>Darpan Anand and Vineeta Khemchandani</i>	
4.1	Introduction	61
4.2	ISO standards for security	62
4.2.1	ISO/IEC 27001 standard	63
4.2.2	ISO/IEC 9798	63
4.3	Authentication, authorization, and access management	64
4.3.1	Identification	64
4.3.2	Authentication	66
4.3.3	Authorization	71
4.3.4	Access management	71
4.4	Policies for identity and access management	77
4.5	Security attacks and goals	79
4.6	Identification and access management techniques	80
4.6.1	Identity management techniques	81
4.6.2	Access management techniques	82
4.7	Identity and access management of e-healthcare systems: case study	82
4.7.1	IoT-based healthcare security	82
4.7.2	Smart e-health gateway	85
4.7.3	Implementation components for the e-health care system	85
4.8	Summary	88
	References	89
5	Application design for privacy and security in healthcare	93
	<i>Arjun Khara, Dharmesh Singh, and Deepak Kumar Sharma</i>	
5.1	Introduction	93
5.2	Understanding EHR systems	94
5.2.1	What is an electronic health record	95
5.2.2	Structure of electronic health record	95
5.2.3	Actors in an electronic health record system	96
5.2.4	Requirements from an electronic health system	96

5.3	Solutions for EHR development	99
5.3.1	Compliance	99
5.3.2	Encryption techniques	100
5.3.3	Access control	100
5.3.4	Identity-based encryption	102
5.3.5	Key management	103
5.3.6	Digital signature and verification	104
5.4	EHR system framework	105
5.4.1	Advantages of cloud	105
5.4.2	Organization of EHR frameworks	106
5.4.3	Cloud-based electronic record systems	107
5.5	Blockchain for EHR systems	111
5.5.1	Problems with centralized architectures	113
5.5.2	Blockchain overview	114
5.5.3	MedRec	119
5.5.4	Storing data off chain	120
5.5.5	Identity and claims	121
5.6	Conclusion	125
	References	126

6 Sustainable future IoT services with touch-enabled handheld devices 131

Davinder Rathee, Kiran Ahuja, and Anand Nayyar

6.1	Introduction	132
6.2	Emerging IoT technologies	133
6.2.1	Wi-Fi (wireless fidelity)	134
6.2.2	Bluetooth	134
6.2.3	Zigbee	134
6.2.4	LoRaWAN	135
6.2.5	Z-wave	135
6.3	IoT architecture for diverse solutions	135
6.4	Real-world application areas of IoTs	141
6.4.1	Healthcare	141
6.4.2	Smart home/office/buildings	142
6.4.3	Wearable	142
6.4.4	Logistics and supply chain management (SCM)	142
6.4.5	Transportation	143
6.4.6	Alerts for disasters	143
6.4.7	Smart agriculture	143
6.5	The role of handheld devices in IoTs	143
6.6	IoT networks versus handheld devices networks	144
6.6.1	Required long battery life	144
6.6.2	Network scalability in heterogeneous environment	144
6.6.3	Required low deployment and adaptability cost	145

6.7 Opportunities and challenges of IoTs with handheld devices	147
6.8 Conclusion and future scope	148
References	148
Part II Healthcare models, solutions, and security standards	153
7 Existing enabling technologies and solutions to maintain privacy and security in healthcare records	155
<i>C. Eben Exceline and Jasmine Norman</i>	
7.1 Introduction	156
7.1.1 Contributions	157
7.1.2 Organizations	158
7.2 Existing technology	158
7.2.1 Cloud computing	158
7.2.2 Fog computing	160
7.3 Security requirement for EHR	160
7.3.1 Data integrity	160
7.3.2 Interoperability	160
7.3.3 Data privacy	161
7.3.4 Fine-grained access control	161
7.3.5 Availability	161
7.3.6 User privacy	161
7.3.7 Scalability	161
7.3.8 User revocation	161
7.4 Attacks over EHR	162
7.4.1 Destruction and modification	162
7.4.2 Denial of service	162
7.4.3 Disclosure	162
7.4.4 Repudiation	162
7.4.5 Masquerading	162
7.4.6 Insider attack	162
7.4.7 Spoofing attack	163
7.5 Maintaining security and privacy of EHR in existing technologies	163
7.5.1 Symmetric key encryption	163
7.5.2 Public key encryption	164
7.5.3 Identity-based encryption	165
7.5.4 Attribute-based encryption	165
7.5.5 Multiauthority attribute-based encryption	166
7.5.6 Hierarchical attribute-based encryption	168
7.5.7 Attribute set based encryption	168
7.5.8 Hierarchical attribute set based encryption	170
7.5.9 Comparison of various encryption techniques	171
7.5.10 Various authentication schemes	171
7.6 A recent development to maintain privacy and security of EHR	174
7.6.1 Blockchain technology	176

x *Security and privacy of electronic healthcare records*

7.6.2	Advantages of blockchain over EHR	177
7.6.3	Comparison of cloud computing and blockchain	177
7.7	Conclusion	178
	References	178

8 Healthcare models and algorithms for privacy and security in healthcare records **183**

Bandana Mahapatra, Rajalakshmi Krishnamurthi, and Anand Nayyar

8.1	Introduction to data security in healthcare	184
8.2	Healthcare overview	186
8.2.1	Healthcare evolution	186
8.2.2	Healthcare information security	187
8.2.3	Need to implement privacy in healthcare data and information	187
8.2.4	Health security as a public health concept	188
8.3	Security issues in healthcare data and information	188
8.4	Models for healthcare security	191
8.4.1	RBAC healthcare model	192
8.4.2	Task role-based access control model	194
8.4.3	HL7 role-based access control model	195
8.4.4	Attribute role-based access control model	196
8.4.5	Privacy access control model for e-healthcare service	196
8.4.6	TMAC model	197
8.4.7	Security model for healthcare in cloud computing	198
8.4.8	Security model for healthcare in big data	200
8.4.9	Security model for healthcare in wireless sensor network	201
8.4.10	HIPAA privacy rules	203
8.5	Introduction to algorithms for security and privacy of healthcare system	203
8.6	Data storage security	204
8.6.1	Threat analysis	206
8.7	Data access security	208
8.7.1	Public key cryptography	209
8.7.2	Data sharing security	212
8.8	Authentication	213
8.9	Conclusion	215
8.10	Future scope	216
	References	216

9 Information security and privacy in healthcare records: threat analysis, classification, and solutions **223**

Arjun Khera, Dharmesh Singh, and Deepak Kumar Sharma

9.1	Introduction	223
9.2	Threats to information security and privacy	225

9.2.1	Understanding information security and privacy	225
9.2.2	Classification of threats	225
9.3	Information security and privacy disciplines	227
9.3.1	Information access control	227
9.3.2	Statistical disclosure control	229
9.4	Models and algorithms	230
9.4.1	Information access control	230
9.4.2	Statistical disclosure control	237
9.5	Conclusions and future directions	242
	References	244
10	Safety measures for EHR systems	249
	<i>Deverajan Ganesh Gopal and Udhayakumar Hari Haran</i>	
10.1	Introduction	250
10.1.1	Traditional record maintenance in EHR	250
10.1.2	Electronic healthcare report	251
10.2	Terminologies	252
10.2.1	Safety and effectiveness of EHR	252
10.2.2	Safety imperfections in EHR	253
10.2.3	EHR safety steps	253
10.2.4	Using EHR as a tool in health care process	253
10.3	Medical record maintenance	254
10.3.1	Implementation and design of safe EHR	254
10.3.2	Achieving performance in EHR using safety testing and reporting mechanism	255
10.3.3	Managing and preventing EHR-related flaws	255
10.4	Medical data breach	256
10.5	Technical issues	257
10.5.1	Storing and preserving the storage of records for long pursuit	258
10.5.2	Synchronization of records	259
10.5.3	Customization of HER	261
10.6	eHealth and teratology	262
10.7	Building a safety EHR safety metrics	262
10.8	Conclusion	263
	References	263
11	Protection framework and safety standards related to electronic health records	267
	<i>Isabel De la Torre Diez and Aránzazu Barbey-Alvarez</i>	
11.1	Introduction	267
11.2	Framework for the protection of personal information in the healthcare context	269

11.3	Special protection for sensitive data and prohibition of the processing of personal data	269
11.4	Medical data processing by a professional	270
11.5	Safety standards in EHRs	271
11.6	Security for healthcare communication	272
11.7	Case study: implementation of a secure EHRs system in the cloud	272
11.8	From the optional computer to the cloud	273
11.9	Application implemented completely in the cloud	275
11.10	Conclusion	279
	References	279
12	Security and privacy issues in UK healthcare	283
	<i>Neetesh Saxena, Robin Singh Bhadoria, Sara Dickerson, Sophie Branch, Lucy Dalley, and Natasha Churchill</i>	
12.1	Introduction	283
12.1.1	Scope and context	283
12.1.2	Security and privacy issues in healthcare infrastructure	283
12.1.3	Challenges in resolving S&P issues	284
12.2	Detailed problem analysis	284
12.2.1	Security attacks	284
12.2.2	Privacy attacks	285
12.2.3	Impact on enterprise	285
12.3	Proposed solution	285
12.3.1	Overall solution description resolving discussed S&P issues	285
12.3.2	Resistance against security attacks	287
12.3.3	Resistance against privacy attacks	288
12.4	Conclusion and future directions	288
	Appendix A	289
	References	299
Part III	The role of blockchain to maintain security and privacy in healthcare	303
13	Blockchain-based health information privacy protection	305
	<i>Quanxin Zhao</i>	
13.1	Basic concepts	306
13.1.1	Health information	306
13.1.2	Health-related data privacy	306
13.1.3	Blockchain in healthcare	306
13.2	The process of health information and data	306
13.2.1	Participants in healthcare and e-healthcare	306
13.2.2	Authentication and access for health data	306

13.2.3	Storage and maintenance in health data	307
13.2.4	Protection and recover for health data	307
13.2.5	Case studies in health information privacy	307
13.3	Laws, policies, and standards	311
13.3.1	Privacy legal protection with laws	311
13.3.2	Practical examples of privacy policies	311
13.3.3	Standards in the area of privacy and security	312
13.4	Healthcare IT systems	313
13.4.1	Current privacy in healthcare IT systems	313
13.4.2	Technical solutions to secure privacy	313
13.4.3	IT security challenges and case studies	313
13.5	Blockchain solutions for health information privacy	315
13.5.1	Blockchain impact on health information privacy	315
13.5.2	Technological frameworks	316
13.5.3	Performance evaluation metrics for security and privacy	316
	Further Reading	317
14	The importance of healthcare information privacy through blockchain	321
	<i>Dhananjay Kumar, Sharmila Arun Kumar, Pramod Kumar, and Mohd Helmy Abd Wahab</i>	
14.1	Introduction	322
14.2	Blockchain: how it works?	324
14.3	The general architecture of blockchain integrated healthcare data management system	326
14.4	Privacy and integrity of healthcare data: challenges and issues of utilizing blockchain	331
14.4.1	Design improvements	332
14.4.2	Data storage requirements	332
14.4.3	Data privacy and protection	332
14.4.4	Communication scalability-based healthcare systems	333
14.5	Healthcare data management: scope for tightening security offered by blockchain	333
14.5.1	Technical advancement in the fundamental principles of blockchain	335
14.5.2	Ethereum	336
14.5.3	Hyperledger	338
14.6	Potential uses of blockchain technology in healthcare industry	338
14.6.1	Prescription and supply tracking of narcotics drugs	339
14.6.2	Flexible data exchange between parties	339
14.6.3	Patient controlled healthcare services	339
14.6.4	Learning ecosystem development for decision making	340

14.6.5	Digital identification of the patient	340
14.6.6	Insurance claims reimbursements	341
14.7	Future research directions of utilizing blockchain in healthcare	341
14.8	Summary	342
	References	342
15	Enhancement of health-care services using blockchain with data authentication and protection	345
	<i>Bharat Prajapati and Satyen Parikh</i>	
15.1	Introduction	345
15.1.1	The laws of privacy	346
15.2	History of concerning issues	347
15.2.1	Traditional health-care system	347
15.2.2	History of health care	348
15.2.3	History of data protection	349
15.2.4	History of blockchain technology	349
15.2.5	Transaction of blockchain life cycle	350
15.2.6	In what way blockchain technology could transform our lives	352
15.3	System design	352
15.3.1	Security principle	352
15.3.2	Distributed network	353
15.3.3	Patients	355
15.3.4	Doctors	356
15.3.5	Internet service provider	357
15.3.6	Health-care industry	357
15.3.7	Cloud	357
15.3.8	Insurance agency	358
15.3.9	Pharmaceutical industry	358
15.4	The blockchain-based health-care industry	359
15.4.1	Benefits of health-care blockchain	362
15.4.2	Challenges of health-care blockchain	364
15.5	Future trends	365
15.6	Conclusion	366
	References	366
16	Blockchain-powered healthcare insurance system	369
	<i>Hardik Gajera, Manik Lal Das, and Viral Shah</i>	
16.1	Introduction	369
16.2	Preliminaries	373
16.3	The proposed system	375
16.3.1	Description of the protocol	377
16.3.2	Medical reports uploading	379

16.3.3 Policy claim against treatment	380
16.4 Analysis and discussions	381
16.5 Conclusion	384
References	384
17 Conclusion	389
<i>Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar</i>	
Index	391

This page intentionally left blank

About editors

Dr. Sudeep Tanwar is an Associate Professor in the Computer Science and Engineering Department at Institute of Technology, Nirma University, Ahmedabad, Gujarat, India. He is visiting Professor in Jan Wyzykowski University in Polkowice, Poland and University of Pitesti in Pitesti, Romania. He received B.Tech in 2002 from Kurukshetra University, India, M.Tech (Honor's) in 2009 from Guru Gobind Singh Indraprastha University, Delhi, India and Ph.D. in 2016 from Mewar University, Chittorgarh, Rajasthan, India with specialization in Wireless Sensor Network. He has authored or coauthored more than 100 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, Wiley, etc. Some of his research findings are published in top cited journals such as IEEE Transactions on TVT, IEEE Transactions on Industrial Informatics, Applied Soft Computing, Journal of Network and Computer Application, Pervasive and Mobile Computing, International Journal of Communication System, Telecommunication System, Computer and Electrical Engineering and IEEE Systems Journal. He has also published six edited/authored books with International/National Publishers. He has guided many students leading to M.E./M.Tech and guiding students leading to Ph.D. He is Associate Editor of IJCS-Wiley and Security and Privacy-Wiley. His current interest includes Wireless Sensor Networks, Fog Computing, Smart Grid, IoT, and Blockchain Technology. He was invited as Guest Editors/Editorial Board Members of many International Journals, invited for keynote Speaker in many International Conferences held in Asia and invited as Program Chair, Publications Chair, Publicity Chair, and Session Chair in many International Conferences held in North America, Europe, Asia and Africa. He has been awarded best research paper awards from IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019.

Sudhanshu Tyagi is an Assistant Professor in Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Deemed University, Patiala, Pb., India. He is visiting Professor in Jan Wyzykowski University in Polkowice, Poland. He received his Bachelor in Engineering in Electronics & Tele-Communication in 2000 from North Maharashtra University, Jalgaon, Maharashtra (India). He achieved second rank in the university at under graduation level. He received his Masters in Technology with Honor's in Electronics & Communication Engineering in 2005 from National Institute of Technology, Kurukshetra, Haryana (India). He received Ph.D. in 2016 from Mewar University, Chittorgarh, Rajasthan (India). He has 50 research publications in peer reviewed journal and conferences from leading publishers like Elsevier,

Springer, Wiley etc. He is reviewer for the board of international journal from leading publisher like International Journal of Ad-Hoc and Ubiquitous Computing, Inderscience and Journal of the Franklin Institute, Elsevier. His research area includes lifetime enhancement of homogeneous and /or heterogeneous WSNs. He is a member of IEEE and IAENG.

Prof. (Dr.) Neeraj Kumar is currently working as full Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, (Deemed to be University), Patiala, Punjab, India. He received his PhD in CSE from Shri Mata Vaishno Devi University, Katra (J&K), India. He was a postdoctoral research fellow at Coventry University, Coventry, UK. He has published more than 300 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, etc. Some of his research findings are published in top-cited journals such as IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCC, IEEE TKDE, IEEE TVT, IEEE TCE, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE SJ, FGCS, JNCA, and ComCom. He has guided many PhD and ME/MTech. His research is supported by fundings from Tata Consultancy Service, Council of Scientific and Industrial Research (CSIR) and Department of Science and Technology. He was awarded best research paper awards from IEEE ICC 2018 and IEEE Systems Journal 2018. He is leading the research group Sustainable Practices for Internet of Energy and Security (SPINES) where group members are working on the latest cutting edge technologies. He is a TPC member and reviewers of many international conferences across the globe. He is visiting professor at Coventry University, Coventry, UK. He is a senior member of IEEE. He has more than 6000 citations and current h-index of 42 (updated August 19). He has edited two books from Springer and IET. He is an Associate Technical Editor of IEEE Communication Magazine. He is an Associate Editor of IJCS, Wiley, JNCA, Elsevier, Computer Communications, and Security and Communication, Wiley. He has been a guest editor of various International Journals of repute such as - IEEE Access, IEEE Communication Magazine, IEEE Network Magazine, Computer Networks, Elsevier, Future Generation Computer Systems, Elsevier, Journal of Medical Systems, Springer, Computer and Electrical Engineering, Elsevier, Mobile Information Systems, International Journal of Ad hoc and Ubiquitous Computing, Telecommunication Systems, Springer and Journal of Supercomputing, Springer. He has been a workshop chair at IEEE Globecom 2018 and IEEE ICC 2019 and TPC Chair and member for various International conferences.

Preface

The Numerous challenges of Healthcare 4.0 environment using electronic medical record (EMR) technology such as data management, human interfaces, scalability, security and privacy, and interoperability have been explored in this book. EMR helps the healthcare providers to make smart decisions during time-critical healthcare service. It also helps to safeguard the sensitive data with less delay as compared to a standalone application like PHR. The Healthcare Industry revolution, PHR system evolution, and its pitfalls in terms of security and privacy of data and development of EMR have been discussed in the introduction. In addition to this, the patient-centric EMR system with data security and privacy is also discussed in the introduction. To show the effectiveness of patient-centric EMR model, different aspects such as application environments of EMR has been discussed in different chapters. For example, what are the privacy issue and how to handle it? What are the security issues and probable solution to resolve it? How to provide quality of services (QoS) to the patient with security on healthcare data? How to ensure scalability and computing efficiency? How to deal with the development and implementation of an EHR system?

The book is organized into three parts: first part is focused on technological development in healthcare, which includes five chapters. The second part discussed the healthcare models, solutions and security standards, which has six chapters. Finally, the last part illustrates the role of the latest technology “blockchain” in healthcare with well-structured four chapters. Lastly, the book has concluded the research work done so far in EMR technology various aspects of security and privacy.

Part I: Technological developments in healthcare

The chapter “Introduction to healthcare information privacy and security concerns” highlights the various security and privacy concerns related to EHR. This chapter highlights the research gaps of traditional systems such as handwritten prescription and manual record keeping over the electronic system by presenting a systematic comparison. It also covered the challenges behind the adoption of EHR such as financial, technological, and interoperability challenges.

The chapter “Fundamentals of healthcare system and general rules for security and privacy” is providing a comparison between traditional medical care system and manual record keeping system. It also highlights the problems occurred due to security and privacy breach of EHR system. This chapter incorporates the HIPAA act mentioning the privacy and security rules for EHR in healthcare.

The chapter “Identity and access management system” discussed how IAM provides security to the EHR records and how it is important to implement it in healthcare industry over the financial industry. This chapter explained the basic and technical concepts of IAM along with the ISO security. Further, various techniques and applications are also explained which are required to understand the concept of IAM. Lastly, few case studies have been discussed along with the IAM implementation components for healthcare system.

The chapter “Application design for privacy and security in healthcare” aims to highlight the purpose of EHR system, identify the shortcomings, and mandatory system requirement. It also discusses the various methods which can address the aforementioned shortcomings. Some security and privacy aspects of cloud-based EHR systems and their implementations were also discussed. Finally, this chapter has presented the implementations of blockchain-based solutions and is suited for EHR systems.

The chapter “Sustainable future IoT services with touch-enabled handheld devices” presents the integration of mobile devices with IoTs and also mentioned its challenges and opportunities with real-world applications. It also discussed the role of cloud environment in mobile devices. Authors have focused on communication aspects of HER and enlighten the 5G communication system. 5G system has the capability to reduce the delay and increase the reliability in records fetching.

Part II: Healthcare models, solutions, and security standards

The chapter “Existing enabling technologies and solutions to maintain privacy and security in healthcare records” explore the current trends and technology to handle privacy and security issue for healthcare data with respect to Cloud and Fog computing. It shows a significant concern to outsource the cloud services to maintain EHR privacy and security. Several encryption techniques have been included in this chapter to encrypt EHR with data integrity. It is difficult to achieve a significant amount of data privacy in a cloud computing paradigm. Hence, the author implies the blockchain technology, where each transaction in EHR is transparent, auditable, and traceable; thus, it provides data integrity.

The chapter “Healthcare models and algorithms for privacy and security in healthcare records” aims to cover three key approaches namely, *data storage, access, and authentication*. These approaches are focused to maintain the digital healthcare records so that patient’s records are kept safe using CIA principle. The chapter also focuses on various algorithms that are connected to the above three approaches to maintain the security and privacy in healthcare IT. The development and implementation of an enhance EHRs system is as of now constrained and not open to most human services associations. Discussion of security-related aspects in healthcare, working of various healthcare models implementing security and privacy and different algorithms used for data storage and access to security and privacy are also covered. This study focused on the enhancement of the EHR system with the aim that no patient is hurt by an EHR.

The chapter “Information security and privacy in healthcare records: threat analysis, classification, and solutions” presented the classification of threats, its analysis and existing solution. In this chapter, several aspects of healthcare are explored. Also, focuses on how a well-designed information system could revolutionize healthcare services while potentially saving billions of dollars. Further, discuss that a HIS or EHR cannot be implemented without giving special thought to information security and privacy infrastructure. It is also evident peculiar problems regarding information privacy and security and innovative and custom solutions for them. In this chapter, numerous categories of threats to a health information system are presented and identified threats that are unique to a health information system. Later, the authors explored numerous models and algorithms that may be utilized to lessen these threats. Finally, proposed future directions which will encourage researches into this field.

The chapter “Safety measures for the EHR system” talks about safety procedures. The development and implementation of an enhance EHRs system is as of now reserved and not open to most healthcare service providers. Hence, the chapter focuses on this part so that social insurance associations, medicinal services providers, security engineers, EHR merchants and assessors, and human components engineers can provide better services to the patients. Aforementioned different parties can work together in one integrating environment of EHR with the goal that no patient is hurt or feel insecure pertaining to their personal data.

The chapter “Protection framework and safety standards related to EHRs” corresponds to a practical application of a secure HCE system in the cloud at the Vega Baja Hospital in San Bartolome (Orihuela, Alicante). Authors discuss the safety standards and security rules for better communication in the EHR system. Here, the case study shows the cloud-based application implementation. The chapter shows the data storage system permits a safe-fast solution. The proposed solution in this chapter displayed the working of EHR system on the web server.

The chapter “Security and privacy issues in UK healthcare” identifies the privacy-related risk and its solutions. It describes the information flow from data collection, use of data, which the user has access to the data and other contacting methods. It shows the identification of a privacy issue and the privacy risk related to the identified scenario. Further, identifies the privacy solution for different privacy issue. For this, privacy impact assessment (PIA) is conducted for data protection and records the PIA outcome and integrates the PIA outcome back to the project plan for better results.

Part III: The role of blockchain to maintain security and privacy in healthcare

The chapter “Blockchain-based health information privacy protection” explores the blockchain technology and its framework in terms of privacy and security in e-healthcare system. This chapter also gives deep insight into the laws, policies, and ISO standards of e-healthcare system. Authors have discussed the challenges of healthcare system and how a blockchain helps to mitigate those issues. Finally, this

chapter discusses the case study which shows the validation of blockchain in healthcare.

The chapter “The importance of healthcare information privacy through blockchain” highlights the concern of blockchain in healthcare system to mitigate security and privacy issues. This chapter discussed that the blockchain offers an interoperable platform for data management which is almost not possible in centralized system. It also depicts the potential of blockchain in healthcare system with its potential characteristics.

The chapter “Enhancement of healthcare services using blockchain with data authentication and protection” discusses the concerning issues in healthcare. This chapter gives deep insight into the blockchain terminologies and its security and privacy aspects in e-healthcare system. Authors also highlight the core component of healthcare blockchain technology, benefits of healthcare blockchain, challenges of healthcare blockchain, and future trends.

The chapter “Blockchain-powered healthcare insurance system” discusses the usage of blockchain technology in EHR. Authors present protocols that address the issue of ill-formed medical report for availing/denial of health insurance. The protocols use blockchain technology that ensures accountability and transparency of services availed by different entities involved in the healthcare insurance system. Patient can avail deserving service from the insurance company and the insurance company can confirm the legitimacy of the medical report by using these proposed protocols. The protocols are shown secure in standard security model and the implementation of these protocols can be done in any existing blockchain platform such as Hyperledger and Ethereum.

The editors are very thankful to all the members of IET Publication, especially Prof. Joel J P C Rodrigues, Series Editor for giving us the opportunity to edit this book.

Dr. Sudeep Tanwar, Ahmedabad, Gujarat, India

Dr. Sudhanshu Tyagi, Patiala, Punjab, India

Dr. Neeraj Kumar, Patiala, Punjab, India

Part I

Technological developments in healthcare

This page intentionally left blank

Chapter 1

Introduction

*Sudeep Tanwar¹, Rajesh Gupta¹, Aparna Kumari¹,
Sudhanshu Tyagi², and Neeraj Kumar³*

From the last two decades, different trends in industry applications and standards have been observed by the communities across the globe. Industry 1.0 was focused on Mechanical Engineering and modernization followed by industry 2.0, which was dominated by Electrical energy sector. Then comes industry 3.0 having information communication technology (ICT) as its major components. But, with the development of Internet of thing (IoT) and Cloud computing (CC), the current generation of Industries, i.e., industry 4.0 depends on the insightful deployment of smart devices such as smartphone, smart watches, smart meters, and their utilization. Advancements in Industries provides interaction between billions of smart devices across the world. Like other Industries (Electrical, Civil, or Mechanical), Healthcare industry also goes from different phases from 1.0 to 4.0. Figure 1.1 shows the growth of the Healthcare industry from industry 1.0 to industry 4.0. To make eco and the user-friendly environment worldwide, Healthcare industry should comprised of administration accessibility in comparison to the other different Industries as mentioned above. Healthcare industry is still in its infancy as it signified its start in the year 1970. The efforts made then were fundamental, and assets were constrained, so, that stage was called as Healthcare 1.0. Subsequent advancements in information technology (IT) field and development of medical technologies such as tracking system, medical imaging conveyed Healthcare 2.0 in the picture. The initiation of new and compelling treatment strategies has begun with having data processing systems and computational intelligence techniques. In this direction, Healthcare 3.0 come up in mainstream because of the usage of electronic health records (EHR) from 2006–2015 [1]. EHR is an alternate form of patient's data chart. This phase has embraced the EHR to help specialists to get significant data on time. The revolution in Healthcare Industries is as shown in Figure 1.1. Strong communication technologies and artificial intelligence (AI) in

¹Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmadabad, India

²Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala, India

³Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, India

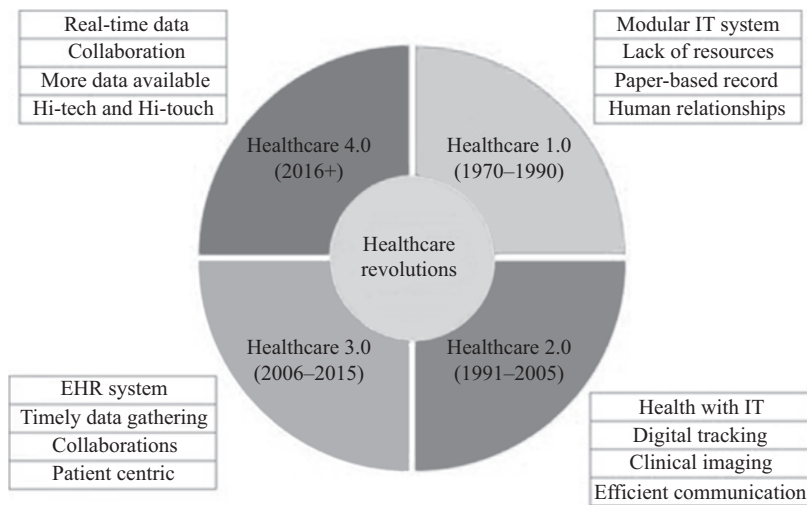


Figure 1.1 Healthcare industry revolution

Healthcare system provide efficient and useful analytic to specialists/physicians [2]. These value-based systems empower Healthcare industry in providing well-informed decisions with the quality of service (QoS). Medical service in the United States is considered as Healthcare 4.0 where 90% of the Healthcare system has been intended to turn toward the value-based system. In India, it is relied upon to keep running the healthcare industry with an expected spending of 6,000 million US\$ by the year 2020 [3]. Several Healthcare IoT gadgets are generating a lot of data at regular intervals. So, security and privacy to such data are key issues. Physical storage of data at hospitals/clinics or any other place may raise the security and privacy concerns of the patients [3].

1.1 Personal health record

With the integration of ICT and hospital information system (HIS), EHR, and personal health record (PHR) have been used across the globe. PHR is a collection of appropriate information relevant to a patient’s wellbeing. It may include (i) a list of healthcare providers involved in the patient’s diagnosis, (ii) diagnosis list, (iii) contact information of patient and his family members, (iv) immunization history, (v) allergy list, (vi) family medical history, and (vii) medications list. Some PHRs are independent PHRs, where patients fill in the data from their very own records and memories. These data are stored on the patients’ PCs or on the web. Patients can choose whether to import the data to relatives, healthcare providers, or any other individual associated. In a few cases, data can be taken from diverse sources into the PHR. Fastened, related PHRs, are connected to a particular medicinal services association’s framework or a healthcare data framework termed as EHR. The patient gets access to the data through a protected gateway. Normally, patients can

see data, for example, lab results, vaccination history, or due dates for specific follow-ups. These are called connected/tethered PHRs. At the point when a PHR is associated with the patient's lawful medical record, it is ensured under the Health Insurance Portability and Accountability Act (HIPPA) Privacy Rule [4].

While an individual health record (PHR) gives an electronic record of the customer's wellbeing-related data, the thing that EHRs maintained and managed by practitioners and kept up by professionals, the PHR is administered by the customer. PHR empowers every customer to view, control, and secure the information and offers it with different parties when required. PHR may contain data from various sources, for example, doctors, home monitoring gadgets, and other information out-fitted by the customer. PHR has several issues to manage the data by itself such as difficulties in the integration of health data with other parties due to data formats. It has another issue such as redundancy because required information to be up to date on frequent intervals and have security and privacy issue while sharing data.

1.2 Privacy and security issue in PHR

One of the important issue for PHRs is how this technology can protect the privacy of patient's health information. Network communication issue is another common problem [5], thus to store an individual medical information online can be a source of the exposure of sensitive health information to unauthorized entities [6]. Medical records can expose critical information in addition to height, blood pressure, weight, and other quantitative data regarding a patient's physical body. The critical personal data such as surgical procedures, fertility, diseases, emotional disorders, and psychological disorders, which lots of patients are hesitant to share [7].

Several attacks may exist related to the confidentiality of patient information as follows.

1.2.1 *Insider curiosity and subordination*

Medical healthcare personnel may misuse the given access for personal benefits such as spite, profit, revenge, or other purposes by leaking the patient information out [8].

1.2.2 *Accidental disclosure*

All through there are several digital transfers of data to numerous entities, healthcare providers can make mistakes to cause data to expose [8].

1.2.3 *Outsider intrusion*

Hackers, network intruders, previous employees, or others may steal or access information, disrupt operations, damage systems, and steal hardware [8,9].

1.2.4 *Uncontrolled secondary usage*

Patient information exclusively used for the purpose of providing primary care, but it can be exploited for reasons that are not mentioned in the contract, for example, research [10].

To handle the aforementioned issues, an EHR system has been introduced in the healthcare industry 4.0 to provide better security and privacy to a patient's health data [11].

1.3 Electronic health record

An EHR is a digital version of a patient's paper-based records of health. EHR is a patient-centric system, which makes data available instantaneously and securely to the official users in real-time. It does contain the medical histories of patients, also go beyond the clinical data collection and give a broader insight into a patient's care. EHRs allow access to the evidence-based tools to make accurate and precise decisions for patient's care. Also, it automates and streamlines the workflow to service providers. It also contains diagnoses procedure, medications and treatment plans, immunization dates, allergic information, radiology images, and laboratory test results. One of the major criteria of EHR is that health data can be generated and managed in digital format by the authorized providers. The medical staff of EHR system uses to record data in the forms of text, graph, symbols, charts, and other electronic data generated by HIS. These electronic data items can be managed, transmitted, stored, reproduced, and replicated efficiently. With the incredible evolution of the acceptance of EMR, different clinical data such as diagnostic history, medications, lab test reports, demographics, vital sign, and so on are getting to be accessible. This sets up the EMR as a fortune gem for data analysis of health data.

EHRs are used to share data with other health care organizations for instance specialists, pharmacies, medical imaging facilities, laboratories, emergency facilities, and providers for instance clinics. Hence the information is gathered from all clinicians to provide better health care to a patient. Information shared in these records should be protected by law and to the authorized users only.

The EHRs facility of data sharing with different organization raises the security and privacy concerns of the patients. Figure 1.2 shows the complete

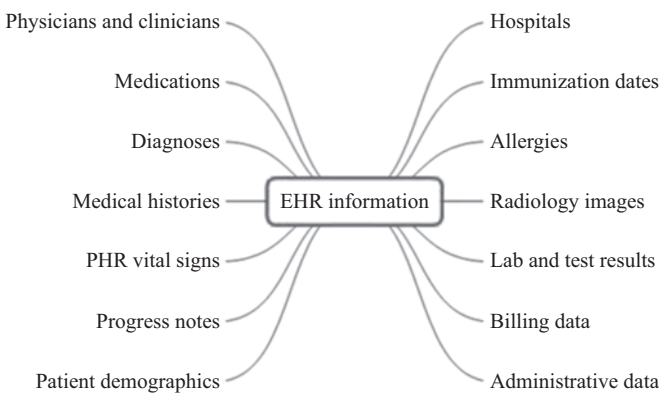


Figure 1.2 Type of information

architecture diagram for the security and privacy issue in EHR. A patient has the full rights that health information is to be stored in paper format or in the electronic form. The federal law is applicable to the information lies with the EHRs [12].

1.3.1 Advantages of having EHRs

Regardless of whether the healthcare supplier is simply beginning to change from paper records to EHRs or is as of now utilizing EHRs within the workplace, we explored at least one of the accompanying advantages. It can be categorized in two categories (i) according to patient and (ii) healthcare providers. Following are the advantages for the patient category.

1.3.1.1 Enhanced quality of care

Specialists/Physicians using the EHRs may think that it's simpler or quicker to follow the patient's lab results and offer advancement with the patient's and other providers. It provides an ease to everyone to work together to make sure that the patients are getting the proper care. For instance, medication information is available on EHR for every patient so that the physicians don't give medicine to patients that can be harmful in combination with the existing running medications. If a patient has an accident, EHR helps emergency doctors or physicians to understand the patient's medical history, while the patient is unable to explain health history. The hospital can get the health issues, medication, and tests report instantly so that the emergency care can be faster and well-formed.

1.3.1.2 More convenient care

EHRs can alert providers to contact patients for follow-ups, to track test reports, and share a health progress report with patients. If we have a sharing system like EHR, multiple doctors can see the information at the same time and the test doesn't need to be repeated. For example, If a PSP patient has a fall and has a fracture in the bone then patient need the treatment from the multiple doctors such as neurologist and orthopedics at the same time to handle the disease properly. It is convenient for the patient and the caregiver both to access all data conveniently at the same time. Patients no need to fill the same data in different forms to let the doctors know the case.

1.3.1.3 Save efforts and time

EHR helps to save lots of efforts and time of both patients and caregiver. It provides the facility to the caregiver to treat the patient at a fast pace.

According to healthcare Providers category, following advantages are identified [13]:

- Quick management of the electronic messaging such as email, text message, chats and telephonic calls for appointments and medicine refills
- Decrease chart tugs
- Upsurge intracommunications amongst offices of different care providers
- Remote access of patients information

- Empower quality and efficient assured medical practices
- Reduce tedious and repetitive task
- Improvement financial system for billing
- Reduction in different kind of errors such as paper errors and human errors cost
- Decrease chemist's call back and increase formulary compliance prescription

1.4 What are the benefits of EHR technology?

The utilization of the EHR system is currently the standard working procedure in healthcare industry 4.0 for all types and sizes of organization. Supported by the establishment of EHR applications, it offers many key advantages for experts, medical staff, and customers:

- Providing access to extensive, current, and accurate exact customer data at the point of care
- Accurate, faster, and convenient prescription of medication
- Enhancing patient's safety by reducing diagnostic errors and improving accuracy
- Enabling the security and privacy of patients medical information within multiple providers
- Increasing efficiency in administrative areas such as billing and collections, scheduling of appointments
- Benefit organization in lower business-related costs
- Facilitating good communication between patients and the care providers [14]

1.5 Security and privacy concern in EHR

Security and privacy are the foremost concern for growing individual trust and data integration. The health information of patient's/individuals should be secure and private within the healthcare provider and individual and for getting the healthier result. The patients hesitate to disclose his/her health information if he/she doesn't have trust in the EHRs system. Hence, security and privacy of health record play a crucial role because leaking of health data of patient could create the life threatening consequences.

Security and privacy is required between patient and physicians/doctors. A model on Security and Privacy is as shown in Figure 1.3. The EHR generates medical data from different data sources such as patient's warbles, smartphones, caregivers, in-patient monitoring, PHR system, and so on. Once data is generated, it is stored in the local databases and then stored at the remote system using a remote gateway. As soon as we collected the data and store it and further share it, the possibility of attacks and privacy issue starts here. To mitigate this, various privacy preservation techniques need to be applied. Some of the examples of privacy techniques are shown here such as grant access, access control model, and pseudonymity. Further, some attack mitigation techniques are mentioned such as authorization and authentication.

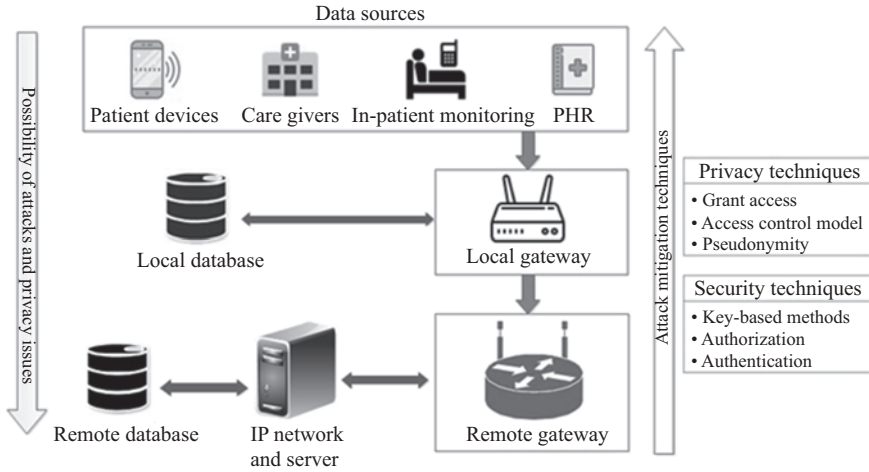


Figure 1.3 Security and privacy model in EMR

To recover from disease, the patients need to share their personal information such as blood pressure, height, weight, previous medical history with doctors for diagnosing the disease, and to take the right actions for treatment. In a few situations such as patient is suffering from HIV or psychiatric disorders, patients reluctant to share their information because it may lead to social scrape and prejudice [15]. In addition to the present medical information of patients, correspondingly collection of other information is required such as the patient's identification for instance personal information, past medical judgment, digital representation of medical images, previously medical treatment taken from which doctors, drugs-history, heredity disease information, genetic disease information such as hemophilia, diet-habits, sexual liking, psychological outlines, history of employment and earnings, personal and mental state among others [16].

1.5.1 Privacy in EHR

Privacy is the rights of any individual who keeps his data with himself, not reveal to others [17]. The claim on the data by an individual should be alone not from another person, any organizations, or government [18]. The information which is shared on the costs of medical relationship should be secured and protected because it is measured as confidential [18]. The data such as diagnoses results, laboratory test results, identification information, and progress reports are stored in different forms like images, text, video, etc. The patient's information regarding his/her can't be disclosed in most of the case such as patients have prostate cancer [18].

The patient's information can be released as per law or only after a patient's permission. Nevertheless, it is not like, the specialist can't access patient information without the permission of patients during treatment. The doctor can view a patient's data for treatment and share to the administrator for payment purpose.

The patient's himself also having full rights to view copy or update the data regarding his health. Following are the privacy techniques available to handle the privacy issue in HER.

1.5.1.1 Grant access

Concealment makes sure that only accredited person can access the health data. It also provides the process of access that is the limitation to the user for getting health data. At the healthcare provider side, the administrator first recognizes the number of users, the access level of health information based on role and privileges for each user. Further, assign a username and password to every user. For instance, the doctor and receptionist have different work and responsibilities, so they can't have the same access rights to access the same information.

1.5.1.2 Access control model

Access control model and authorization present the most difficult challenge in the implementation of EHR systems. EHR should ensure the healthcare information should never be visible, accessible, and modifiable by unauthorized individuals or organizations. An identity management system is typically composed of three major elements: users, systems/applications, and policies. The access control policy dictates the interactions of users with the system. It is typically based on the privilege and right of each practitioner authorized by the patient or trusted third parties. There are broadly two access control models, role-based access control (RBAC) [19] and attribute-based access control (ABAC) [20,21]. To solve this access problem, first is to store the records in the centralized system under the protection of the party managing the databases. Then, a fine-grain level for access in this centralized system is achieved by access control methods. These methods typically store healthcare data in an unencrypted form and the access control protects the system from unauthorized access and acts as a firewall. The other substitute is to merge the information encryption with access controls. It ensures data integration and authorized access, so providing both security and privacy as the healthcare data are stored in an encrypted format. This is possible by engaging the cryptographic access control (CAC) model with the centralized system. It helps to construct composite EHR consisting of data from multiple sources. Table 1.1 shows the comparison of different access control methods with their feasibility. These methods are RBAC which defines a class of roles and access levels, ABAC which is refined access control model and provides tremendously fine-grained control over the access policies and the last one is CAC which requires a central authority referred to as a reference monitor for mediating access.

1.5.1.3 Pseudonymity

It is the anonymous identity, in which the user has a reliable identification in the EHR system that is not a real name: a pseudonym. Pseudonyms are typically names chosen by the user. Real identities are only accessible to system administrators in the pseudonymous system. Pseudonymity allows users to communicate with each

Table 1.1 Comparison of access control models

Parameters	Customization	Levels of anonymity	Execution efficiency	Scalability
Role-based access control	Low	Low	High	High
Attribute-based access control	High	High	Low	Low
Cryptographic access control	High	High	High	High

other in a commonly anonymous way without worrying for securities. It helps to maintain privacy and security.

1.5.2 Security in EHR

Subsequently, from the emerging EHR, security is one of the major concern for healthcare information. Nowadays, the use of smart devices such as smartwatches, wearables, mobile phones, and so on has been increased exponentially. Typically, the transaction of healthcare information within clinicians, patients, and federal agencies are also increasing the theft of medical identity.

The patients can loose their trust in the doctor if he faced data theft. To maintain patient's trust, medical record should be protected. The medical staff, doctors, and other parties involved in the treatment should be aware of security standards to secure patient's data and data within medical practices.

As per the survey, 73% of doctors write text messages to other doctors regarding their work [22]. While transmitting the text, security is the foremost concern in EHR. It is very difficult to control communication which is interrupted by a rival, where data and images are transferred and shared. The devices are used for secure transfer by encrypting the text. The mobile devices are used and it cannot design for centralized management [23]. The terminals are hardly lost; conversely mobile can be misplaced, damaged, or stolen. Hence, it is important to use encrypted mobile devices to transfer confidential information.

To avoid probable threat for instance hacking, alteration, or damage of data by internal or external users, training programs of security standards must be completed by users. The antivirus software's firewalls and intrusion detection software should be used as a security standard to protect data. Furthermore, to maintain the data integrity for full security programs are installed in the system. As well as an audit trail should be monitored to check who had to access the patient's data.

To track the system activity audit trails are used with time and date for every entry, details viewed by which users and how long system being accessed, manage logs of all alteration in records [24]. The administrator can get the details of screenshots, printed reports, and track the computer location. It can be prevented from violators but cannot prevent the EHR system from data disclosure and unauthorized access.

1.6 Challenges in security and privacy

It is compulsory to assure the patient's privacy against the risk associated with EHR [25].

1.6.1 Verification of user

Merely authorized user has right to admittance healthcare records. Several authentication systems such as token-based and biometric-based authentication systems should provide assurance to the users for authorized access to healthcare records [26].

1.6.2 Integrity and confidentiality

It provides accuracy and reliability to healthcare records as well as reliability and integrity of the computer system and communication system. The alteration of data and harm of health records may be done by the hacking of EHR [27].

1.6.3 Access control

It is vigorous issues of security to share health records stored in databases. The rights of each user and their role are differently constructed as per the organization and system need. Consequently, it is compulsory to control rights of each user for accessing the resources. It is tough to identify a user who is retrieving the data in nonsecure remote connection [28]. The EHR system requisite the features for security such as role wise access of the system, authentication system and audit trails.

1.6.4 Data control

It is important to reflect at the time when the distribution of rights to admittance patient's data. Right of authority on healthcare data, user access which healthcare data, as well as transparency on the healthcare system, should be accomplished in ownership of healthcare records [29].

1.6.5 Data security policies

The security policy is implemented because many organizations are involved during medical treatment. Every organization has to decide the limitations of its function in advance. The healthcare organization has to choose stringent rules and processes for inhibiting from loss or theft of portable devices and physical media. EHR system must regularly get updated their functionality to handle blockage in right to use of labs result, track of visioning, encrypt entries, manage security with increasing level [30].

1.6.6 Profiles of user

Many entities for instance patients, doctor, medical organization, druggist, etc. are involved in the health care system. Hence, as per the role of users, variations in functionality and security levels should be there [21]. It is challenging to identify every

patient within different units due to incompatibility in the EHR system. There is the requirement to match record by record which creates interoperability within units [31].

1.6.7 Misuse of health record

The privacy is challenging when the EHR system uses the free storage space from different third parties. In this case, mishandling of data is possible and can be happened by sharing or selling it to other organizations. The security of healthcare data is a thought-provoking task in multispecialist situations [32].

Finally, standard law and federal organization are required to notify the patients and other healthcare providers such as doctors and hospitals about the breach. This requirement let the patients know if something has gone wrong with his data and helps the providers accountable for the protection of EHR data.

References

- [1] Hathaliya J.J., Tanwar S., Tyagi S., and Kumar N. (2019). "Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach." *Computers & Electrical Engineering*, vol. 76, 2019, 398–410.
- [2] Vora J., Tanwar S., Verma J.P., *et al.* (2018). "BHEEM: a blockchain-based framework for securing electronic health records." *2018 IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, pp. 1–6.
- [3] Kumari A., Tanwar S., Tyagi S., and Kumar N. (2018). "Fog computing for Healthcare 4.0 environment: opportunities and challenges." *Computers & Electrical Engineering*, 72, 1–13.
- [4] <https://www.healthit.gov/sites/default/files/factsheets/about-phrs-for-providers.pdf>
- [5] Office of the National Coordinator for Health Information Technology (2016). "Breaches of unsecured protected health information." Health IT Dashboard. Retrieved July 3, 2018. <https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php>
- [6] Cerrato P. (2017). "Medical data breaches: the latest health care epidemic." GW Public Health Online Blog. Milken Institute School of Public Health, George Washington University. Retrieved July 3, 2018. <https://publichealthonline.gwu.edu/healthcare-data-breaches/>
- [7] Weitzman E.R., Kelemen S., Kaci L., and Mandl K.D. (2012). "Willingness to share personal health record data for care improvement and public health: a survey of experienced personal health record users." *BMC Med Inform Decis Mak*, May 22, 2012, <https://bmcmmedinformdecismak.biomedcentral.com/articles/10.1186/1472-6947-12-39>.
- [8] <https://www.beckershospitalreview.com/healthcare-information-technology/top-3-security-threats-to-the-healthcare-industry-tips-to-avoid-them.html>
- [9] Le Bris A., and El Asri W. (2017). "State of cybersecurity and cyber threats in healthcare organizations: applied cybersecurity strategy for managers" (PDF). ESSEC Business School. Retrieved July 3, 2018.

- [10] Health Information and Quality Authority (2012). “International review of secondary use of personal health information” (PDF). Health Information and Quality Authority. Retrieved July 3, 2018.
- [11] https://en.wikipedia.org/wiki/Personal_health_record
- [12] <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf>
- [13] Vora J., Dev Murari P., Tanwar S., Tyagi S., Kumar N. and Obaidat M. S. (2018). “Blind signatures based secured E-healthcare system.” *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Colmar, France, pp. 1–5.
- [14] <https://www.psytechsolutions.net/emr-vs-ehr-vs-phrs>
- [15] Applebaum, P.S. (2002). “Privacy in psychiatric treatment: threats and response.” *American Journal of Psychiatry*, 159, 1809–1818.
- [16] Mercuri, R.T. (2004). “The HIPAA-potamus in health care data security.” *Communications of the ACM*, 47(7):25–28.
- [17] Warren S.D., and Brandeis L.D. (1890). “The right to privacy.” *Harvard Law Review*, 4:193.
- [18] Rinehart-Thompson L.A., and Harman L.B. (2006). “Privacy and confidentiality.” In Harman LB, ed. *Ethical Challenges in the Management of Health Information*. 2nd ed. Sudbury, MA: Jones and Bartlett. p. 53.
- [19] Science Applications International Corporation (SAIC). Role-based access control (RBAC) Role Engineering Process Version 3.0. May 11, 2004.
- [20] Mohan A., and Blough D.M. (2010). “An attribute-based authorization policy framework with dynamic conflict resolution.” *Proceedings of the 9th Symposium on Identity and Trust on the Internet*.
- [21] Hagner M. (2007). “Security infrastructure and national patent summary.” In *Tromso Telemedicine and eHealth Conference*.
- [22] Greene A.H. (2011). “HHS steps up HIPAA audits: now is the time to review security policies and procedures.” *Journal of the American Health Information Management Association*, 82(10):58–59. <http://www.ahimajournal-digital.com/ahimajournal/201110?pg=61#pg61> [Accessed August 10, 2012].
- [23] American Health Information Management Association. (2012). “Mobile device security (updated).” *Journal of the American Health Information Management Association*, 83(4):50. [Accessed August 10, 2012].
- [24] American Health Information Management Association. (2008). Copy functionality toolkit; 2008:4. http://library.ahima.org/29%3Cand%3E%28xPublishSite%3Csubstring%3E%60BoK%60%29&SortField=xPubDate&SortOrder=Desc&dDocName=bok1_042564&HighlightType=PdfHighlight. [Accessed August 10, 2012].
- [25] Vora J., Italiya P., Tanwar S., *et al.* (2018). “Ensuring privacy and security in E-health records.” *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Colmar, France, pp. 192–196.
- [26] Han Y., and Deng B. (2004). “A smart-card-enabled privacy preserving E-prescriptions system.” *IEEE Transaction on Information Technology in Biomedicine*, 8(1):47–58.

- [27] Katzenbeisser S., and Petkovic M. (2008). "Privacy-preserving recommendation systems for consumer healthcare services," *2008 Third International Conference on Availability, Reliability and Security*, Barcelona, pp. 889–895.
- [28] Huda M.N., Sonehara N., and Yamada S. (2009). "A privacy management architecture for patient-controlled personal health record system." *Journal of Engineering, Science and Technology*, 4(2).
- [29] Vucetic M., Uzalac A., and Gligoric N. (2011). "E-health transformation model in Serbia: design, architecture and developing." *International Conference on Cyberenabled Distributed Computing and Knowledge Discovery*, IEEE Computer Society.
- [30] Medeiros A. (2002). "Anonymous E-prescriptions." WPES'02, November 21, 2002 Washington, USA. ACM1-58113-633-1/02/0011.
- [31] Riedl B., Grascher V., Stefan Fenz, and Thomas Neubauer. (2008). "Pseudonymization for improving the privacy in e-health applications." *IEEE 41st Hawaii International Conference on System Sciences*.
- [32] Guide to Privacy and Security of Electronic Health Information. (n.d.). Retrieved from <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>.

This page intentionally left blank

Chapter 2

Introduction to healthcare information privacy and security concerns

Anoop Kumar Pandey¹

A systematic collection of electronic health information of individuals (Electronic Health Record or EHR) in general has been picking up lately. We are gradually leaving behind the extensive paper trail along with the illegible handwriting of many physicians and a headache to compile the patient history from the pile of papers. EHR presented itself with several benefits including cost reduction, easy data maintenance and interpretation, use of one's medical history as a reference for similar cases, data sharing, finding trends or correlations in medical histories to detect an anomaly or maybe a cure. To offer these benefits, an EHR system should have properties like high availability, failure resilient, data completeness, secure and privy among others. While numerous benefits are being offered by EHR, given the insecurities in the digital world, it is easily threatened by hackers, worms, viruses and similar attackers. These issues may arise during storage of data, communication of data and use of data. Though several standards and policies like ISO 13606 and ISO/TR 20514 exist citing various guidelines associated with EHR, but individual implementers may choose to put them aside or may not be even aware of them. We would outline such different security and privacy issues while using electronic health records in this chapter.

2.1 Introduction to electronic health records

To ensure quality patient care, the health care industry has been evolving a lot. While most of the developments may be in the discovery of various medicines and development of various tools for diagnosis and treatment, a swift transition to the digitization of patient information viz. complaint, test reports, diagnosis and prescriptions, etc. brought about a plethora of benefits to all stakeholders. Paper-based records had many disadvantages specifically their illegibility, storage and organization, information loss in case of disaster, lack of facilities to share data and many more. Electronic health records (EHR) brought about several changes to the

¹Centre for Development of Advanced Computing (C-DAC), Bangalore, India

system. Ease of access, interpretation, management, maintenance, sharing and compilation of patient health records, generation of research problems, are few of them [1]. Most significantly, the use of historical data as a reference and for finding trends and correlation between data for diagnosis, detection of anomaly and treatment could garner impeccable improvement in health care quality. A complete EHR could also empower the patient to self manage chronic diseases.

2.1.1 Paper-based records

Since time immemorial, hospitals and doctors have been giving handwritten or template-based prescriptions, test/scan reports and any such documents. These paper-based records were primarily used for clinical, research, financial and administrative purposes. To understand the scale of the documents that we may get, a simple case of pregnancy may be considered. From the conception till birth, there are three rounds of antenatal profile tests containing 30+ tests, multiple scans including Dating Scan, NT Scan, Anomaly Scan, Interval Growth Scan, Term Scan and many more, multiple visits and prescriptions. If some complications arise, there are another set of tests and procedures like Double Marker, Quad Marker tests, amniocentesis, etc. Then, in some cases, there may be referral letters, fit to fly certificate and several other documents. Just imagine a bundle of all these reports and prescription and you need to juggle through them if you are looking for something specific or if you are taking second or third opinion in case of complications. This is an example of one event in one's life; just consider the scale of medical records from birth till death.

The transition from paper-based records to electronic health records may be advocated based on the following observations:

- Most of the handwritten prescriptions are illegible (see Figure 2.1 for a sample handwritten prescription). Even if a clinician uses a template, the handwritten fillings of the data are mostly illegible. While it appears prejudiced to say that doctors usually don't have the best handwriting; maybe it's due to paucity of time, or perhaps it's just a matter of habit, but a doctor's note is generally difficult to comprehend by people not belonging to the medical profession. In a recent incident, the High court of Allahabad, India, held three doctors' illegible notes as an obstruction in court work and fined them [2].
- Paper-based records are expensive to copy, share, store and transport.
- Paper-based records are difficult to maintain and store for years. Paper, in general, is prone to destruction or decay. Environmental factors like moisture may damage it. Rodents like mice or insects like termites may chew and waste them. Human error, like misplacement, deliberate destruction, etc. is another enemy of the long life of papers. According to a study [3], 25% of the times, paper charts are missing and the physician has to reorder a test. Natural disasters like fire, flood, etc. may also threaten the longevity of paper records.
- As illustrated above, while understanding the patient's history, going through the bundle of paper records is not only time consuming and cumbersome, taking inference from the history or analysing it is also challenging.

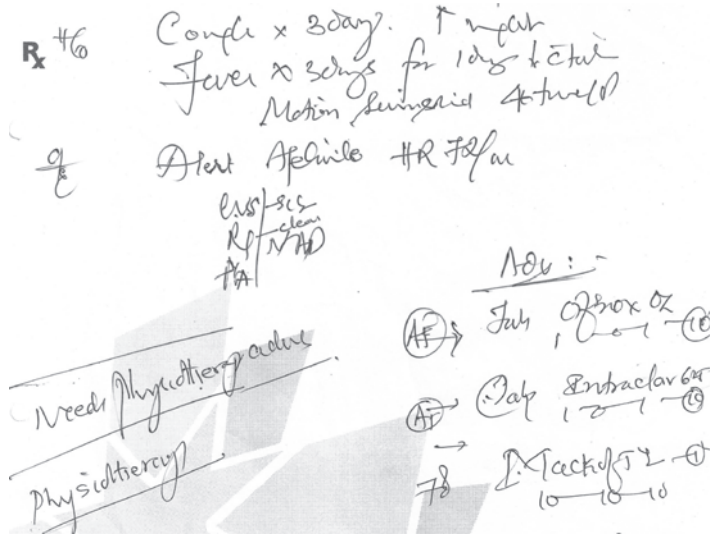


Figure 2.1 A sample handwritten prescription

- It is difficult to figure out the access records (who has seen it!) of the paper-based records. This may elevate privacy concerns.
- Even though paper-based records may be scanned and shared electronically; since it is not a structured data, performing any computation or rule-based inference is not possible on it.
- Another point to consider is the impact of papers on our environment. While we want to move toward a green environment, sticking to paper records may appear hypocritical.

2.1.2 Moving toward EHR

Electronic health records are picking up pace lately over paper-based records. In fact, digitization and computerization have been adopted by almost every field and domain. With medicine adopting the same, this could offer a plethora of benefits to all stakeholders viz. patients, doctors, healthcare institutions, health informatics, etc. So, let's go through the benefits that EHR offers:

- EHRs are better organized than paper records (see Figure 2.2 for HER-based prescription). Easy and fast access of any record, faster search and chronological navigation of patient history enhances the standard of medical care being provided. Instead of going through a stack of papers, now it's just a few clicks. Of course, it will save lots of time and effort improving efficiency and productivity of the healthcare institutions as well.
- Electronic records can be simultaneously accessed by a radiologist, doctors, billing clerks, etc. There is no manual transfer/interchange required.

- Sharing of data is fast and easy, given that the data are globally accessible with just network connectivity. One may easily share his test records and history with insurers to negotiate better deals.
- Copies of data may be easily created. This will not only serve redundancy purpose in case of disaster or loss of data but can also be distributed with multiple stakeholders without any financial overhead.
- Templates for data filing may help doctors remember if they are missing any details to be taken or prescribed. Data completeness will be ensured in this case. In this way, medical errors can be reduced by significantly improving the accuracy of records. This will also save healthcare institutions loads of money by reducing claims arising from malpractice suits. Also, now the prescriptions are legible.
- Online appointments, viewing test reports without going to hospitals and tracking health information, visit and test schedules are so much easier with EHR. EHR can send alerts and reminders for visit, test, medicine refill, etc. and settings for the same can be customized as well.
- EHR data can be easily integrated with other services and systems. An integrated data mining software can provide essential analytic and inferences for

diagnosis and medical breakthroughs. Integration with medical research facilities may provide ample input and sample data for a decision support system and identifying important and urgent research problems. Integration with government data may provide important statistical medical data which may be used to address booming health issues and also help in budget allocation toward public healthcare infrastructure and medical research facilities. Integration of data with insurance service providers may help them in deciding optimal pricing.

- EHR data can be easily aggregated from different sources (hospitals, clinics, diagnostic centres, etc.) and serve as one high-quality data for making an evidence-based decision. This also helps in referrals and coordinated care where multiple physicians, specialists and diagnosticians work together on one patient without any communication gap.
- A complete EHR could also empower a patient to self manage chronic diseases.
- EHR increases the security and privacy of patient data.
- There are multiple health risk assessment tools (e.g. [4]) based on EHR which give recommendations for maintaining a healthy lifestyle based on your test results, charts, vitals and daily activities. This ensures better preventive care for individuals.
- EHR can be stored and archived for a very long period in contrast to the paper-based record which has a limited shelf life.

The above enlisting is not exhaustive but indicative only. Table 2.1 shows a vis-a-vis comparison of EHR and paper-based records.

Table 2.1 Table depicting few of the vis-a-vis comparison of EHR and paper-based records

Features	EHR	Paper-based records
Organization	Complete and systematic	Random
Sharing	Fast, efficient, economical	Cumbersome and costly
Accessibility	24*7, parallel access	Limited, no parallel access
Search	Fast	Slow
Loss or misplacement of records	Rare	Frequent
Maintenance	Easy	Difficult
Illegibility	None	Might be
Analysis	Easy	Difficult
Security	High	Low
Environmental impact	Low	High
Impact of disaster	Low	High
Alerts, reminders	Yes	No
Compliance	Yes	May/may not
Archival	Indefinitely long	Paper shelf life

Government of India initiative toward electronic health records

The Ministry of Health and Family Welfare (MoHFW), Government of India, is setting up an Integrated Health Information Platform (IHIP). The primary goal of IHIP is to create standards compliant Electronic Health Records of the citizens across the country. This centralized platform will ensure the interoperability of the EHRs through a Health Information Exchange (HIE). IHIP is intended to offer better medical data management, proper information exchange, reduction in human-induced errors, security, confidentiality, better decision support system, thereby improving level of care, disease diagnosis and management, affordability and ultimately country wide enhanced treatment of public health. MoHFW has already issued Electronic Health Record Standards (EHR Standards) [5]. Also, the rules of Clinical Establishments (Registration and Regulation) Act, 2010, notified on 23 May 2012, mandates maintaining and sharing of EHRs with the Government from time to time. [6]. Additionally, MoHFW vide National Health Policy 2017 emphasized on medical records digitalization aiming to establish an integrated health information system with colligating and interoperability of the EHRs across both public and private health facilities.

2.2 Components of an EHR

There are multiple components (functionalities) and stakeholders in an EHR. Standardization has also helped in deciding which key features could be important enough to be added in an EHR (Figure 2.3).

2.2.1 Core components of an EHR

A committee of the Institute of Medicine of the National Academies has identified eight key capabilities of an Electronic Health Record system in order to promote greater safety, quality and efficiency in health care delivery [7].

The eight core functions are as follows:

1. Health information and data (patient's diagnosis, reports, course of treatment, etc.)
2. Result management (provision for accessing old and new test results)
3. Order management (provision for entering and accessing orders for the test, medicine, etc. Computerized Physician Order Entry (CPOE) is generally used for inpatient order entry)
4. Decision support (decision support systems enabling prompts, reminders, alerts for preventive and regular care)
5. Electronic communication and connectivity (seamless connectivity and communication like e-mail facility between the patient, healthcare providers and/or any other stakeholders)



Figure 2.3 Key functionalities of an EHR system

6. Patient support (patients having access to their health record, education about their condition and help for self-managing chronic conditions)
7. Administrative processes and reporting (administrative tools like scheduling or appointment system, etc.)
8. Reporting and population health (standardized data storage and reporting tool for the purpose of public health monitoring or disease surveillance)

2.2.2 Additional desirable capabilities

In addition to the above-mentioned core functionalities, an EHR is expected to have the following features:

- New patient registration system.
- Referral management system for inter and intrahospital referrals.
- Multiple modes of inputting data like typing, voice commands and dictation, templates, etc. are desirable. In the case of handwritten order entry, OCR (optical character recognition) should be there.
- A customizable table summarizing diagnoses, medication, allergies, severity, etc. for ready reference.
- Facility for inpatient, outpatient and international patient EHR adoption.
- Ability to generate certificates like fitness certificate, fit to fly certificate, reimbursement claim certificate, etc.
- Access from ubiquitous devices viz. smartphone, tablet PC, etc.

- Remote access from anywhere, be it office, home, hospital, etc.
- Ability for management and generation of systematic bills. Provision for discounts and reimbursements, as and when applicable, should be there. Integration of digital payment systems in the billing system is also desirable.
- Knowledge Bank (like Medical Wikis AskDrWiki, Clinfowiki, EyeWiki, HemOnc.org, etc. [8]) for ready reference.
- Facility for health risk assessment tool for preventive care.
- Facility for graphical representation and co-relation in treatment and vitals.
- Facility for a fallback system, backup and restore in case of an outage.
- Addressing security and privacy concerns as per the Health Insurance Portability and Accountability Act (HIPAA) standards [9].

2.3 Challenges in EHR adoption

While EHR offers so many benefits and an increase in productivity, still its adoption rate is still very low. There are still many of the hindrances in EHR adoption and it's seamless use.

2.3.1 Technological makeover

Establishing a paper-based health record is pretty simple. Print a bunch of letter-heads and you are good to go. Moving to an EHR requires effort, training, finance, infrastructure, manpower, etc. To establish an EHR, hardware like computer systems, server, printers, scanners, storage, network connectivity, HVAC (Heating, Ventilation and Air Conditioning) system, networking components like switches, routers and access points, and network security equipments like Unified Threat Management (UTM), Firewall, Intrusion Prevention System (IPS), etc. are required. Additionally, an EHR software, database software, productivity software like Office, user web portal and other software components are required. To avoid any failure of the systems, additional backup and fall-back servers and mechanism should be in place. To run and maintain such infrastructure, additional manpower and trained professionals are required. Moreover, the staff and doctors need to be trained on the new technology to have an understanding of the system and the new workflow. A study [10] established that an average end-user would require 134 hours of training to understand and prepare for the implementation. Additionally, a patient may also need a small amount of education to understand and use the system. As number of ubiquitous devices like smartphones and tablets are increasing with multiple platforms like Android and iOS, mobile applications also need to be developed for each platform.

2.3.2 Financial challenge

All the above technological makeover including procurement and implementation would require a lot of funding. The cost implication is not limited to one-time infrastructure establishment cost, but additional recurring cost like maintenance cost, bandwidth cost, additional manpower cost, annual subscription, etc., also, contribute

to the financial challenges in adopting EHR. According to [11], lack of funding has been a prime obstacle in the adoption of EHR. The training of the staff would also contribute significantly to the financial burden in EHR adoption. Furthermore, a study [12] on RoI (return on investment) of EHR adoption reported that only 27% of the practices garnered positive 5-year return and remaining experienced financial loss.

2.3.3 Personnel cooperation

There is nothing new about the reluctance of personnel for any technological change. The reluctance of medical staff appeared to be the second big challenge in EHR adoption [13]. The drastic change in workflow and working system will require a large amount of training and practice for the staff and doctors. With the template-based workflow for CPOE (computerized physician order entry) takes time and in a way, reduce the productivity of the physician as well with an increase in documentation time of 238% [14]. A survey [15] indicated that 20% of respondent practitioners discontinued use of EHR and returned to a cheaper solution or usual paper-based solution.

2.3.4 Interoperability

Different EHR software has been written in different languages and is offered by different vendors. The functionalities that they offer also vary. There is a lack of interoperability standards. Migration of data from one system to another is a cumbersome task. Even in case of an upgrade, if there are multiple components (EHR, billing, scheduling and practice management), the interfaces and ports need to be checked and changed accordingly. It's therefore that buying an all integrated system (EHR + billing software + scheduling software + any other components) is often preferred than buying separate modules.

2.3.5 Integration with other systems

Integration of EHR with different other systems poses another challenge. EHR can be integrated with a data mining tool for providing analytic and other medical inferences. EHR can be integrated with Government data to provide important statistics which could be used for addressing important and grave health issues and also help in decision making toward the building of public healthcare infrastructure. All these integrations require compliance with standards and law. It requires compatibility and interoperability for data sharing and data computation. Additionally, data completeness, data cleansing and data correctness are other important challenges prior to integration with such systems.

2.3.6 Usability

Another issue of usability comes into picture where the ease and efficiency of using the EHR software with organized and intuitive modules is concerned. Usability covers effectiveness (accuracy and completeness), efficiency (speed) and user satisfaction in performing a task. Better user experience with less number of clicks

and entries for searching and completing a task is often desirable. Healthcare Information and Management Systems Society (HIMSS) has defined the following principles for evaluating EHR usability [16]:

- **Simplicity (Si):** Relevant information display, highlighting important information, clutter-free design and easily comprehensible functions constitute simplicity.
- **Naturalness (Na):** Workflow should match the practical life task. Familiarity and intuitiveness also promote naturalness.
- **Consistency (Co):** Not only data but interfaces must also be consistent with one another. Coherent layout and terminologies should be used throughout the application.
- **Forgiveness and Feedback (FoF):** Providing feedback regarding ongoing work, set of options, their meaning and explanations, the repercussions of their usage, etc. should be integral. Tasks, where input data may be inconsistent or actions which may impact the system (like delete data) must come with an alert to the user before proceeding.
- **Effective Use of Language (EUL):** Common and unambiguous language words and phrases comprehensible and being used generally by clinicians should be used in the interfaces.
- **Efficient Interactions (EI):** Minimum set of interactions (like clicks or entries) should complete a task.
- **Effective Information Presentation (EIP):** The information or interface presenting the information must be well organized, easily readable and customizable in some cases.
- **Preservation of Context (PC):** Keeping minimal screen changes and visual interruptions while completing a task.
- **Minimize Cognitive Load (MCL):** There should be minimal use of mental work (minimal calculation, segregation or integration of data, interpretation of functions) to perform a task.

2.3.7 Data completeness and correctness

While the heading may come as a surprise, data completeness and data correctness are major hurdles against EHR. Given that, we are seeking integration of EHR with data analytics software for data mining, we must strive for data quality. There are several dimensions which contribute to data quality; data completeness and correctness are the most crucial among them. Data completeness refer to the collection of all necessary data and information pertaining to a task. Though data completeness is important for analytic, without data correctness, all inferences based on that data will not be valid. Documentation errors may develop consequential and cumulative medical error when another medical practitioner reviews for second opinion or arbitration. He would rather believe documented facts in EHR (even though erroneous) than the patient. Data correctness is also crucial in the sense that an incorrect data or history can lead to the wrong hypothesis, diagnosis, medication and even death in some case. According to a Johns Hopkins study [17], medical

mistakes are the third leading cause of death and have caused more than 2.5 million deaths in the United States alone after heart disease and cancer. Other studies have found this tally higher than 4 million.

Some mistakes are hard to fix! [18]

Morgan Gleason, 19 years old, studies in a college. At the age of 11, she suffered from juvenile dermatomyositis (JDM) which is a systemic autoimmune disease. Fever, rash around the eyelids, elbow and joints, etc., muscle weakness and pain, weight loss and mouth ulcers are the main symptoms of JDM. This disease is very rare and only affects 1 to 3 in a million people per year.

She believes that mistakes in medical records happen often. While minor issues (like marking male as female or pain in the lower back instead of the upper back) won't make a dent in a long go, but we ought to raise it to the doctor for fixing it. However, when major errors appear in one's record, that raises serious concern. A similar incident occurred with Morgan. She was stunned to see diabetes on her health condition list. This was somehow added when a doctor accidentally marked diabetes on an MRI order form and when the specialist sent the notes to the primary physician, he added diabetes to her medical condition. While this may appear like a blunder, the next error was humongous. Her OB (obstetrician) records showed that she had been pregnant twice (one at the age of 13 in 2011) and she has a surviving male child. Considering, it could have been an honest mistake of mixing up of two patient's records, she requested for corrections in the record but office staff responded that if such fact was there, then the patient must have told so. Later she submitted a request for correction in writing and upon confirmation, the corrected copy of the record was sent to her in the mail.

2.3.8 Storage of EHR data

An important consideration in the adoption of EHR is for long-term storage and archiving of patient data. This will also come with planning for information life cycle (storage, deletion, the life-time of data, etc.), accessibility in future if required and physical and virtual security of the data. The required length of the storage of individual data may be governed by the rules and regulations stipulated by the Government or the legislation. The format for data storage (relational, XML, NoSQL, object-oriented, etc.) will also affect the availability and accessibility performances.

2.3.9 Security of EHR data

With EHR, while everything seems to fall in line, the possibility of the exploit of health records in the hands of an adversary could also bring about disastrous consequences leading to financial, social, ethical, legal implications and even loss of life in some case. Security in EHR refers to the protection measures and tools used

to safeguard the patient information from unauthorized access and abuses, manipulations, deletion and denial to access.

I would like to list some of the indicative (not exhaustive) security concerns that should be addressed to avoid a long road of legal tribulations:

- The trivial security concerns of establishing confidentiality, integrity and availability are always there.
- Weaker methods of authentication and authorization may sabotage the entire security goal.
- Physical security of data holding establishments poses another concern.
- The potential for misplacement of data lies during the paper-based system to electronic conversion.
- Data completeness, correctness and verifiability pose another challenge where lack/incorrectness of data may lead to an inconclusive diagnosis.
- Data usage or sharing through ubiquitous devices broaden the scope of security to multiple platforms and communication channels.
- Access through role-based privileges may enhance the security and privacy of data; however, the problem may arise when a user has multiple roles and privileges. For example, a doctor in one speciality (high privileged) may be a patient in another speciality (low privileged) and access should be defined accordingly.

Safety measures like access control, encryption of data or an audit trail may safeguard the data, however, can't guarantee complete protection. Upcoming technologies like blockchain can ensure the integrity of data and proper audit trail, but confidentiality and privacy may still be of concern, given that the blockchain may require to be shared with other medical institutions or practitioners.

2.3.10 Privacy concerns

Richard Rognehaugh defined Privacy as 'the right of individuals to keep information about themselves from being disclosed to others; the claim of individuals to be let alone, from surveillance or interference from other individuals, organizations or the government' [19]. Privacy in healthcare settings refers to people's right to control access to their personal and sensitive personal information. Patient information should be shared with others only with the patient's consent and/or as required by law. When a patient is mentally incapacitated or unable to consent due to age or any medical condition, a next of kin or legal guardian or legal representative may decide upon information sharing. Information can also be released for treatment, payment or administrative use without a patient's authorization. The patient may also view or seek a copy of his/her own medical records or request for an amendment if required. Additionally, a patient should get noticed through the choice of method of contact about how and where his data are being used or shared. Another concern of privacy rises when patient information is shared with another medical institution or practitioner for referral or second opinion. What data to be shared, to whom (speciality or role) should it be shared, at what granular access control model, with what permissions and for how long, are few privacy concerns that should be addressed while sharing patient's data.

There can be several disadvantages to a privacy breach. Public release of health information can also be awkward or embarrassing to a person's social or professional life. Moreover, health insurers can use negative health information to charge particular individuals higher premiums or to deny coverage.

2.4 Security concerns in healthcare information

2.4.1 Physical security

Physical security of the hardware (server, storage, security devices, etc.) holding healthcare information is very important. A data centre may be encroached by individual/individuals for sabotaging it or tampering/stealing the data. An internal member of the organization may also try to modify or steal or delete data if the authentication-based access system is not in place. In another case, poor ventilation and air conditioning may cause devices to burn out due to excessive heating which, in turn, will destroy the data. Natural disasters like fire and flood may also lead to the destruction of the data centre and consequently the data.

The data centre should have a proper HVAC system in place. Security personnel should be present for preventing any unauthorized access to the servers or security devices. The data centre should have an access control system with a combination of an access card, pin and/or biometric features for authentication. It may have CCTV-based surveillance system for monitoring any activity. It should have a fire suppression system for preventing fire accidents.

2.4.2 Application security

EHR records are generally accessed using an EHR software which implements various functionalities ranging from access to addition, modification, sharing and customization. It also has access control along with authentication and authorization. Additionally, there is a patient portal as well, which is usually a web-based application. An EHR software may be written in any of the several programming languages. There may be some design issue, inherent language specific bug, some coding error and some other issues which could compromise the application security. Another source of insecurity is default settings for software. An insecure default setting may lead to serious intrusion and accessibility problem given that most of the end users accept the default settings and rarely customize them for strengthening the security or changing the work-flow. Similarly, the web application may have their own exploitations and vulnerabilities apart from non-secure coding practices [20]. The web or application server (like Apache, Tomcat, JBoss, Glassfish, etc.) hosting the web application may have different vulnerabilities. Many Linux based operating systems update their software repository very late. In such cases, if there is any vulnerability, even if a security patch is released, the OS may take time to install the patch. It is recommended to patch the systems as soon as they are released. Manufacturers and developers should have proper plans for maintenance, management, monitoring, upgrading, patching operations and recovery from an outage (application or OS crash).

2.4.3 Server security

All the data and main application reside in a physical or virtual server. Even if the application is secure, but the operating system of the server is not hardened (secured), the application may be hacked and data may be stolen [21]. Enabling firewall, use of ACL (access control list), TCP Wrappers, proper authentication and authorization are recommended for server security. If the server is virtualized, appropriate settings in the virtualization software must be enabled or made to ensure high availability and dynamic resource scheduling to avoid virtual machine starvation due to lack of virtual hardware resource [22].

2.4.4 Periphery security

A data centre must have hardware-based periphery security for securing all computing resources. Unified threat management (UTM) with security modules and features like intrusion prevention system (IPS), Firewall, Anti-virus, Anti-spam and URL filtering can serve as gateway security for the data centre. Separate Firewall and IPS may also be deployed. Web Application Firewall (WAF) may be used for securing the patient web portal. Hardware or cloud-based Email Security Solution may be used for securing the emails. These devices will maintain the confidentiality and integrity of the stored data and prevent unauthorized intrusions.

2.4.5 Storage and communication security

The EHR data are often stored on servers or in NAS (Network Attached Storage)/SAN (Storage Area Network). There is always a possibility that an adversary gets access to the storage and thereby accesses the data and exploits it. It is therefore often advisable to store data in encrypted form or use full disk encryption. The data may also be intercepted during communication (while sharing or accessing through the web or remote application access) through sniffing or MiTM (Man in the middle attack). An encrypted data or encrypted communication channel helps mitigate these confidentiality problems. Network segmentation in the operating environment may also seize unauthorized access up to an extent.

2.4.6 Ubiquitous device security

A recent survey [23] found that 73% of the physicians message peer physicians about their work. Security of these message exchanges is another concern in EHR protection. Though EHR data are not exposed directly a fragment of messages referencing EHR data is shared. Also, it is difficult to assess the granularity of the information shared (patient or diagnosis details, images, etc.), the security of the network being used for transmission, and security of the device being used for this purpose. Also, it is difficult to monitor individual handheld devices by the IT security team. Furthermore, there is always a risk for mobile devices to be lost or stolen. Therefore it is desirable to encrypt mobile device data and communication (like Whatsapp end to end encryption [24]) even in peer to peer model.

2.4.7 Preserving confidentiality

Apart from encryption, the preservation of confidentiality can also be ensured by ensuring information access to authorized persons. Identifying a set of persons who can access the information is the key to the process of authorization. Amongst the authorized persons, it is crucial to identify what portion of the information is available to whom and what actions (modification, addition, deletion, etc.) are available to be performed by an authorized person. This will ensure proper responsibility and accountability for all the users. Many administrations use username, password-based authentication to access the data. Various password constraints like minimum length, the inclusion of special characters, change of password at certain interval, etc. are employed. The second level of authentication like biometric (finger/eye scan, facial recognition) or OTP (one-time password) is also adopted nowadays. Jigna J Hathaliya *et al.* [25] have suggested a biometric-based authentication system for secure access of patient records by various stakeholders from any location in an open internet environment. Jayneel Vora *et al.* [26] have proposed a method for preserving privacy of clinical data using an authentication framework with varying degree of access method and an encryption technique.

2.4.8 Data integrity

Data integrity is a property that ensures that data are unaltered. Data may be changed intentionally or unintentionally in some circumstances like during data entry or system upgrades or data transfer. Consider a data transfer from one EHR system to another system and unit of one data column is changed (e.g. unit for fever from °C (Celsius) to °F (Fahrenheit)), the unit conversion may breed some errors. Another example may be drop-down lists where, while entering data, choices are limited and in order to fill all information, one or the other option has to be chosen, even if it poorly matches the exact information. There may be some unintentional errors like entering reverse order of the digits (temperature of 38°C written as 83°C) in some input box. In such cases, if the error is not marginal, the EHR system should have an alert system to indicate probable abnormal entry.

2.4.9 Data availability

An EHR system may be targeted using request overloading or possibly denial of service attack. Some unwanted outage like system (server, storage, etc.) crash may also happen. In such untoward situations, the EHR data availability may be affected or be ceased even. Hacking may also bring down data availability. To counter such situations, multiple backups may be taken. These backup systems may run in active-active mode or active-passive mode. In active-active mode, the main system and backup system both work together using a load balancer which distributes the request load across the systems. High availability is automatically ensured in such systems. But, synchronous data syncing between these multiple systems is an important (must) requirement. In active-passive mode, the backup system is put idle; it is brought up once the main system goes down. Fault-tolerance systems may also be used in case of system or storage crash, where hot replacement (replacement

while the system is online) of components can ensure continuous system and data availability.

2.4.10 Audit trail

There is always a question of accountability, in case, something turns haywire. Audit trail records may come handy in such cases. Audit trails log all activities of addition, modification and deletion of entries in an EHR along with the date and time stamp in addition to access logs, authentication logs and any other related system activity logs [27]. HIPAA mandates to main the audit log records for a minimum of 6 years [28].

As per the HIPAA Privacy and Security Rules, employers can be held liable for the activities of their employees. In 2011, it was found that employees of the UCLA health system gained access to celebrities' records without any authorization. UCLA was held accountable for not implementing enough security measures to mitigate the risk of unauthorized access to protected electronic health information. UCLA health system settled this privacy and security violations with the US Department of Health and Human Services Office for Civil Rights (OCR) for a whopping \$865,000 [29].

2.4.11 Mock drills

Mock drill checks the preparedness of the entire data centre in terms of service (working) and security. With all security practices in place, regular testing of the security system should be done in order to make sure that all devices and rules are working properly. Additionally, it may also indicate if some changes or upgrades need to be ensured in order to cater to the current hostile environment. Often, penetration testing and white hat hacking are done to test the security systems.

2.4.12 Data breach and mandatory disclosure

A medical data breach is an intentional or unintentional release of health information data and could include personal health data from electronic health record or billing records from their health care providers or health insurance providers. Criminal intentions are the primary reason for a medical data breach. In February 2015, a National Public Radio (NPR, USA) report claimed that stolen health data are being sold in the black market with varying high prices. The data contain some personal information like social security number, birthday, address and mother's maiden name which may be used for identity theft, blackmailing and even answering secret questions as part of password recovery, etc. Even the companies who lost data are getting blackmailed in the name of keeping the incident secret [30]. In 2015, Katherine Keefe, a Beazley Group leader for breach response claimed that medical records could be valued at USD 40–50, higher than credit card number (USD 4–5) on the black market [31]. UCLA fired 13 employees, suspended 6 others and took

disciplinary action on 6 physicians for prying at personal medical records of Britney Spears for her treatment in a psychiatric unit. Earlier as well, some were fired for snooping on the birth records of Britney's first son in 2005 [32]. In another incident in India, the Health Solutions pathology laboratory, Thane, Mumbai, suffered data leak of over 43,000 patient's electronic medical data including HIV reports in December 2016 [33]. A study in the *Journal of the American Medical Association* claimed that the health data breaches incidents have drastically increased by a factor of 70% annually cumulating to 344 million stolen records in the last 7 years. Approximately 132 million (3/4th of the total lost or stolen or breached data) being breached through hacking or IT (information technology) incidents [34].

In the United States, the HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health) Act require business associates to notify affected individuals of any data breach and even the federal government in case of loss of protected health information [35]. It mandates companies to have written rules and policies for breach notification and that employee should be trained on these procedures.

2.5 Curbing security concerns

There is no panacea for solving the security issues; however, advisory guidelines may be issued to avoid hacking incidents as far as possible. Some of the recommendations may be found as follows:

- All the hardware equipment viz. server, storage, networking equipment like a switch, access point, security equipment like UTM, Firewall, etc. should have appropriate physical security. There should be an access control system (based on PIN, card, biometric or combination of them) for accessing the systems.
- The data centre must be protected using periphery/gateway security devices like UTM, Firewall, WAF, etc.
- All the hardware should be properly maintained under AMC (annual maintenance contract). Upon the end of support, device retirement is encouraged.
- The data centre should have a proper HVAC system in place.
- The data centre should have a proper fire suppression system.
- There should be an additional copy of data (backup) stored at a geographically different location. There should be proper backup and restore mechanism.
- All the software components (application or system) should be regularly patched and updated or upgraded whichever possible.
- In the software, proper identity management for authentication and role management for authorization should be present. Alerts should be generated in case of any unauthorized access.
- Operating system hardening should be done on the servers and end-user systems from where the application is accessed.
- All the data should be encrypted while storing. Full disk encryption may also be used.

- While communicating the data, secure communication modes like https, vsftpd, scp, etc. can be used. Network segmentation is another way to prevent unauthorized access up to a certain extent.
- Standards should be followed while designing and developing EHR software so as to avoid compatibility and interoperability issues.
- Training to staff and physicians, about proper data entry, modification and data safeguarding should be imparted.
- Frequent security audit and mock drills must be conducted to safeguard EHR systems from cybersecurity threats.

2.6 Privacy concerns in healthcare information

Privacy is quite essential in the healthcare industry. Sharing of patient data with patient consent and information of data being shared to whom and at what granularity drive the privacy front. Maintaining patient trust and privacy is the foundation of the success of a healthcare system. A patient may not willingly disclose certain aspects of their health information in the absence of a trusted environment and this could have fatal aftereffects. There are several reported cases in the United States where patients avoided treatment knowing that health data are not private. The count of such cases rocketed to million with diseases including cancer, mental illness, sexually transmitted diseases (STD) and Post-Traumatic Stress Disorder (PTSD).

2.6.1 Major issues driving privacy front

With the increasing adoption of an EHR system, serious issues pertaining to patient data privacy need to be addressed. In the following subsection, some of the major concerns regarding the privacy of the data have been discussed.

2.6.1.1 Real owner of patient data

Who is the real owner or who controls the patient data? There are multiple stakeholders of the patient data viz. the patient, healthcare providers and software professionals maintaining the data. Actually, there is no real owner of the patient data. Instead, all stakeholders have different roles with varying rights and responsibilities to play. For example, a healthcare provider can modify the data, but they shouldn't have the right to delete it. A patient may decide to delete his or her health records, but he can't modify the healthcare provider's entries. Similarly, software professionals don't have the right to destroy data, but they can modify whenever required. While, everyone assumes that the patient is the rightful owner of their health data, in actual, they have very little control over the data. They may be considered custodian or steward of the data. For example, they can't even change any diagnosis if they don't agree with it, but, they have a right to interact with data and ensure accuracy of the data by voicing their opinion in case of any discrepancy. The same goes for health care providers. They also need to maintain the accuracy of the data by not giving full control of the data to the patient; otherwise, the patient may

change the test results or diagnosis for their own benefits like insurance premium reduction or settlement. The health care providers, who actually create the data and have right to modify, have the responsibility to protect the patient privacy and maintain transparency with the patient about their data especially with sensitive medical information like psychological or gynaecological records. Also, when patients have more connection with their data through the patient portal, they get involved in the self-health care and proactively engage in assessing risks toward their health and make efforts to counter them. In this way, the very idea of multiple people sticking to their role with respect to the EHR data pans out toward a common goal of patient care.

2.6.1.2 Social media penetration

While the exposure of patient health data through electronic records are prevalent, the excessive use of mobile and mobile electronic devices also increases the risk of information dissemination through social media platforms viz. WhatsApp and Facebook, though it may be shared in a closed group for convenience. In one incident, a group of nurses used Facebook to share shift change information containing patient-specific information. Information was later shared with their friends violating privacy regulation [36]. Similarly, in another incident, certain staffs of a hospital posted pictures of a patient health record on a social media site.

The problem with sharing through social media is that once a post is made, a permanent digital footprint is created with multiple copies for redundancy. Similarly, befriending a patient may violate patient confidentiality and may bring down healthcare official legally.

2.6.1.3 Sharing data with external entities

Although sharing of EHR data conveniently is one of the major selling point of EHR, the extent of sharing, private data masking, identity masking, etc. are some of the important points driving the protection of patient privacy. The data may need to be shared with insurance service providers, research institution, government agencies, etc. for different purposes. The records may also be disclosed for quality review of the healthcare institutions. In all such cases, EHR providers need to be proactive in sharing the data in anonymous form keeping the medical information data private. They also need to pre-inform the patient about what data are being shared and at what granular level. They must omit user identifying data if necessary. Patients may also have a choice to decline sharing their entire medical data or portion of the medical data with an entity unless legally required.

2.6.1.4 Role-based access and authorization

In one way, privacy can be achieved through role-based access and authorization to handle confidential electronic health records. The user's access will be based on pre-established access credentials along with role-based authorizations. The administrator identifies the user, determines the level of authorization and relevant information to be accessible at that level and assigns login credentials. The users are accountable for the use and misuse of their credentials and actions and implications arising out of the

usage of that credential. All the users will have access to the information they need to carry out their responsibilities. While this method seems ironclad when confidentiality is concerned, complications arise when a person may have different roles in different cases or scenarios. In that case, he may use his higher privilege for unauthorized access. Consider an example, where a doctor in hospital A and speciality S may be a patient in another hospital B or speciality S. If the health data are consolidated for both hospitals or specialities, then the doctor may be able to access records of any person even in hospital B with his credential as a doctor, though as a patient at hospital B, he wouldn't have any rights/privileges except his own medical record. Therefore, instead of role-based access across the entire system, access may be defined per patient data, that is, for a patient, only a set of consulting physicians and primary physician along with nursing staff will have access to the data.

2.6.2 *Privacy laws and guidelines*

2.6.2.1 **Indian context**

Electronic Protected Health Information (ePHI) refers to any electronically generated, stored, shared, sent or received protected health information (PHI). Any medium may be used to store, send and receive the PHI data electronically.

As per the Information Technology Act 2000, data privacy rule refers to 'sensitive personal data or information' (SPI) as the subject of protection, but also refers to 'personal information' (PI) with respect to certain obligations. Sensitive personal information is defined as a subset of personal information. Sensitive information include passwords, physical or mental examination, sexual orientation, financial information viz. credit/debit card details, biometric information and medical history, etc. Personally identifiable data may be one or combination of identifiers including name, address, all elements of date except Year (e.g. date of birth or date of death), PAN/Aadhar/Vote Id/Passport number, vehicle number, license number, image, voice recording, email address, mobile number, bank account number or credit/debit card number, etc.

The patient is considered as the owner of the protected health information including 'SPI and PI' while the healthcare provider only holds the data in trust on behalf of the patient. The mode of storage or transfer of such data is owned by the healthcare provider. The confidentiality of the patient medical data have to be ensured through mandatory regulations and the patient must have control in that. Patients must have sufficient privileges to view their medical records at any time without any limit. However, if, a healthcare professional opines that release of information may endanger the life or safety of the patient or others, then the healthcare provider may be privileged to deny sharing the information to a patient or a representative or any third party concerned [37]. A patient may only have the limited privilege of changing his medical data in terms of corrections or errors in the recorded medical data.

For disclosure of protected or sensitive information, a general consent has to be taken by the healthcare provider from the patient or next of kin as defined by MCI

(Medical Council of India). For non-routine or non-health care purposes, specific consent has to be taken. For national priority activity like communicable or notifiable diseases, details may be shared without the patient's authorization as required by the law.

Healthcare provider should protect and secure health information. They should remove personally identifiable data while sharing patient information. They should inform all the patients about their privacy rights. They must create guidelines, document all privacy policies, ensure implementation of policies, audit and quality assurance, and train its staffs.

Electronic Health Record of a person must be preserved during the lifetime of the person compulsorily. Upon the demise of an individual, the records may be made inactive preferably after three years of the demise. However, the details must not be deleted permanently ever.

In a landmark judgement, the Supreme Court of India, ruling in a petition of Justice K. S. Puttaswamy (Retd.) and Anr v Union of India held the right to privacy as a fundamental constitutional right [38]. A Personal Data Protection Bill, 2018 has been framed by Justice B. N. Srikrishna Committee and submitted in July 2018. The bill has been sent to Law ministry for vetting by MeitY (Ministry of Electronics & IT, Govt. of India). The bill has been drafted in line with GDPR (General Data Protection Regulation) largely. It will introduce a regulatory framework governing data protection in India. It clearly identifies and awards rights on personal data to the owners. It also issues clear directions for data handling or processing entities (institutions or organizations). Health records, personal information like biometric data, sexual orientation, genetic data, password, financial status, etc. have been categorized as sensitive personal information.

2.6.2.2 US context

The HITECH Act, introduced in 2009, presented a new process for certification of EHRs for the first time sponsored by ONC (Office of the National Coordinator for Health Information Technology), in addition to CCHIT (Certification Commission for Healthcare Information Technology) certification. This new certification ensures HIPAA compliance of the EHRs and further support meaningful use. ONC certification includes requirements on confidentiality of data through database encryption, transmission mode encryption, access control through authentication, data integrity, audit trail logs, automatic log off, access in case of an emergency and also addressing HIPAA releases of information. The HITECH Act also helped in fortifying existing HIPAA requirements especially in enforcing HIPAA and breach notifications. Civil and criminal both penalties for Business Associates as well as other covered entities were added for the first time. Civil penalties could go as high as 1.5 million dollars in their most rigorous form. All affected individuals or

entities must be notified in case of a data breach of PHI (protected health information) occurs. United States Department of Health and Human Services (HHS) must be notified additionally if more than five hundred individuals are affected. Selling protected health information is strictly prohibited. Users of EHRs must use HIPAA compliant technology. They should provide physical security and software-based security of data systems and transmission networks including mobile and remote computing. They should also provide proper access control with privileges through defined user roles, authentication using passwords and auditing for accountability and trail. User behaviour must be monitored and managed. Security policies and procedure must be indicated. An effective business continuity plan must be in place covering procedures for responding to and recovering from an outage.

Though EHRs may have introduced some new potential privacy and security threats for patient data, these risks can be easily extenuated with using technology, user training and compliance. Rest assured, technology offer authentication, authorization, audit trail and backup restore mechanism which can easily safeguard EHRs.

2.6.3 Using blockchain for privacy protection

A blockchain is a growing chain of blocks cryptographically connected with each other. Each block is a Merkle root of the previous block and current set of transactions with a timestamp. Blockchains along with special protocols can be used for varying degrees of privacy and (pseudo) anonymity and could be used to enable the protection of healthcare data. For instance, a user could use a blockchain based health information record store and could share only a specific block of the healthcare information chain such as medicine prescription with a pharmacy to purchase medicines. Jayneel Vora *et al.* [39] have described a framework for storing and accessing medical records in blockchain. This framework known as BHEEM, ensures secure access of medical records along with protecting private information of the patients.

2.6.3.1 Homomorphic encryption

‘Homomorphic Encryption’ allows direct computations on ciphertext without having to decrypt it to get the plaintext. Apparently, this can be used to ensure the confidentiality and privacy of the data while computations like search or addition are performed on it. To access the details of the plaintext, a decryption key will need to be known.

zk-SNARKs and Zero Knowledge Proofs (ZKPs) use homomorphic encryption for their cryptographic operations. zk-NARKs is used to encrypt data by Zcash. Decryption keys are shared with intended recipients for decrypting and viewing the data [40].

Youssef Gahi *et al.* [41] describe homomorphic encryption schemes in which database queries are run on the encrypted data directly. However, the performance suffers drastically with a 16-bit multiplication taking more than 24 minutes even when using a simple and insecure homomorphic scheme.

2.6.3.2 State channels

A state channel is a two-way discussion channel between users or user and service (system). Messages usually are transactions like ‘I want to subscribe to a channel for Rs. 25 for a month’. People participating in the discussion sign all the messages for the purpose of non-repudiation. These discussions take place off the blockchain and are quite fast to execute as compared to blockchain based payments. The final amount is settled on the blockchain (like using smart contracts on the chain).

State channels could allow healthcare providers to keep patient data safe and private. All medical information transaction could take place off the blockchain with a reference hash of the transaction being saved on the blockchain.

2.6.4 Protecting patient data privacy

While, many technological tools and solutions may claim to provide total privacy of the data, policies and regulations also play a vital role in ensuring the confidentiality of the private patient data. An audit trail will be able to track the access and modification list for the data. Responsibility and accountability for the healthcare provider to protect the confidential data and removing safe passage for any intentional or unintentional disclosure of the data can also add to the collective efforts for ensuring the confidentiality of the data. EHR standards and privacy-related regulations (as per the law of the country) should be adopted and followed. Data access should be controlled and without authorization, any access should render the data unreadable and generate alert to designated administrators in real-time.

Moving ahead!

Electronic Health records are crucial in creating health information organizations and a worldwide health information network. A paper-based system is plagued with numerous shortcomings. Despite the benefits that EHR offers, several obstacles and concerns persist. However, every technological change requires some effort, patience and investment initially. The subsidy may be provided by the Government for increasing the EHR adoption rate. Small practitioners may also opt for subscription-based (SaaS: Software as a service) EHR software, set up on cloud infrastructure, to avoid bigger financial burden at once.

References

- [1] Greenhalgh T, Hinder S, Stramer K, *et al.* Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. *BMJ*. 2010;341:c5814.
- [2] Allahabad High Court fines three doctors for ‘bad handwriting’. <https://www.timesnownews.com/videos/news/india/allahabad-high-court-fines-three-doctors-for-bad-handwriting/11557> [Accessed October 04, 2018].

- [3] Tang PC, LaRosa MP, Newcomb C, *et al.* Measuring the effects of reminders for outpatient influenza immunizations at the point of clinical opportunity. *Journal of the American Medical Informatics Association*. 1999;6(2):115–121.
- [4] Health Risk Assessment and Trackers. <https://www.apolloprism.com/#tools>.
- [5] Ministry of Health and Family Welfare, GoI. Electronic Health Record (EHR) Standards for India 2016. <https://mohfw.gov.in/basicpage/electronic-health-record-ehr-standards-india-2016>.
- [6] Ministry of Health and Family Welfare, GoI. The Clinical Establishments (Registration and Regulation) ACT, 2010. <http://clinicalestablishments.gov.in/cms/Home.aspx>.
- [7] Key Capabilities of an Electronic Health Record System. <http://www.nationalacademies.org/hmd/Reports/2003/Key-Capabilities-of-an-Electronic-Health-Record-System.aspx>.
- [8] Giustini D. How Web 2.0 is changing medicine. *British Medical Journal Publishing Group*; 2006;333(7582):1283–1284.
- [9] Centers for Disease Control and Prevention. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. *MMWR: Morbidity and Mortality Weekly Report*. 2003;52(Suppl. 1): 1–17.
- [10] Fleming NS, Culler SD, McCorkle R, *et al.* The financial and nonfinancial costs of implementing electronic health records in primary care practices. *Health Affairs*. 2011;30(3):481–489.
- [11] Wang SJ, Middleton B, Prosser LA, *et al.* A cost-benefit analysis of electronic medical records in primary care. *American Journal of Medicine*. 2003;114(5):397–403.
- [12] Adler-Milstein J, Green CE, and Bates DW. A survey analysis suggests that electronic health records will yield revenue gains for some practices and losses for many. *Health Affairs*. 2013;32(3):562–570.
- [13] Brailer DJ, and Terasawa EL. Use and adoption of computer-based patient records. Oakland, CA: California HealthCare Foundation, 2003; p. 1–42.
- [14] Poissant L, Pereira J, Tamblyn R, *et al.* The impact of electronic health records on time efficiency of physicians and nurses: a systematic review. *Journal of the American Medical Informatics Association*. 2005;12(5):505–516.
- [15] American Academy of Family Physicians. EHR meaningful use dropout rate soars in 2012. <https://www.aafp.org/news/practice-professional-issues/20130703mudropoutrate.html>. [Accessed July 03, 2013].
- [16] Healthcare Information and Management Systems Society (HIMSS). What is EHR usability. <https://www.himss.org/what-ehr-usability/>.
- [17] Study Suggests Medical Errors Now Third Leading Cause of Death in the U.S. https://www.hopkinsmedicine.org/news/media/releases/study_suggests_medical_errors_now_third_leading_cause_of_death_in_the_us [Accessed May 03, 2016].
- [18] Gleason M. Medical record errors. <https://morgangleason.com/> [Accessed February 17, 2017].

- [19] Rognehaugh R. *The Health Information Technology Dictionary*. Aspen Publishers: New York; 1999.
- [20] OWASP Top 10 - 2013. The ten most critical web application security risks. 2013.
- [21] Stallings W, Brown L, Bauer MD, *et al.* *Computer Security: Principles and Practice*. NJ: Pearson Education; 2012.
- [22] Pearce M, Zeadally S, and Hunt R. Virtualization: issues, security threats, and solutions. *ACM Computing Surveys (CSUR)* 2013;45(2):17.
- [23] Greene AH. HHS steps up HIPAA audits. *Journal of AHIMA*. 2011;82 (10):58.
- [24] WhatsApp security: end to end encryption. <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf>.
- [25] Hathaliya JJ, Tanwar S, Tyagi S, *et al.* Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach. *Computers & Electrical Engineering*. 2019;76:398–410.
- [26] Vora J, Italiya P, Tanwar S, *et al.* Ensuring privacy and security in e-health records. In: *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*. Colmar, France. NJ: IEEE; 2018. p. 1–5.
- [27] Gelzer R, Hall T, Liette E, *et al.* Copy functionality Toolkit: a practical guide: information management and governance of copy functions in electronic health record systems. Chicago, IL: AHIMA; 2012.
- [28] Washington L. Managing health information in mobile devices. *Journal of AHIMA*. 2012;83(7):58–60.
- [29] Health and Human Services (HHS). University of California settles HIPAA privacy and security case involving UCLA Health System facilities. HHS gov. 2011;7.
- [30] Shahani A. The black market for stolen health care data. <https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data> [Accessed February 13, 2015].
- [31] Abelson R, and Goldstein M. Anthem hacking points to security vulnerability of health care industry. <https://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html> [Accessed February 5, 2015].
- [32] Ornstein C. Hospital to punish snooping on Spears. <https://www.latimes.com/archives/la-xpm-2008-mar-15-me-britney15-story.html> [Accessed March 15, 2008].
- [33] HIV patients' data in 43,000 path lab reports leaked online. <https://timesofindia.indiatimes.com/city/mumbai/HIV-patients-data-in-43000-path-lab-reports-leaked-online/articleshow/55761372.cms> [Accessed December 03, 2016].
- [34] Tindera M. Government data says millions of health records are breached every year. <https://www.forbes.com/sites/michelatindera/2018/09/25/government-data-says-millions-of-health-records-are-breached-every-year/> [Accessed September 25, 2018].

- [35] HIPAA Breach Notification Rule. Federal Register 2009b. 2016;74:163. Available from: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>.
- [36] Ayres EJ. The impact of social media on business and ethical practices in dietetics. *Journal of the Academy of Nutrition and Dietetics*. 2013;113(11): 1539–1543.
- [37] Data Ownership of EHR: The Ethical, Legal, Social Issues (ELSI) Guidelines. https://www.nhp.gov.in/data-ownership-of-ehr_mtl.
- [38] The Supreme Court of India COJ. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors. Right to privacy. <https://www.sci.gov.in/pdf/jud/ALL>
- [39] Vora J, Nayyar A, Tanwar S, *et al*. BHEEM: a blockchain-based framework for securing electronic health records. In: 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, UAE. NJ: IEEE; 2018. p. 1–6.
- [40] Hopwood D, Bowe S, Hornby T, *et al*. Zcash protocol specification. Technical Report, 2016–1.10. Denver, Colorado: Zerocoin Electric Coin Company; 2016.
- [41] Gahi Y, Guennoun M, and El-Khatib K. A secure database system using homomorphic encryption schemes. arXiv preprint arXiv:151203498. 2015.

Chapter 3

Fundamentals of health-care system and general rules for security and privacy

Hiral Patel¹, Meghna Patel¹, and Satyen Parikh¹

3.1 Introduction

In today's world, there is rapid growth in health-care industry on the conversion of patients' records into electronic form. The main problem raised in an existing system is the way it works. For example, the patient first needs to understand the health issue based on symptoms that are involved in health-care system. When a patient wants to pursue health-care system, the process is repeated for collecting relevant information, interpreting and identifying functioning diagnosis. To understand health problems of a patient, physical supervision, execution of conversation, medical history and symptomatic testing, and consulting with other doctors are different ways for collecting information related to issues of patient's health. In addition, the existing health-care system is afflicted by many issues such as patient's diagnoses written in an enigmatic way on paper, difficulties in obtaining an access to information of a patient, as well as limitations of space, time workforce needed to supervise patient's health. The growth in technology provides the personification of services as well as reduces health-related issues and improves the opportunities in existing health-care industry. In past eras, health-care industry implemented internet and used it to publish information regarding common health, and helped patients expand knowledge for medical disorders using that information. Nowadays, the American Hospital Association have about 5,000 member institutions that have websites to provide detailed information regarding their services and facilities.

3.1.1 *What is EHR (electronic health record)?*

Electronic health record (EHR) is used to create and manage health records of patients in a digital format [1]. It works like a central repository to store patient's health status information. Information such as medicines, medical treatment such as operations, historical information of past diagnosis, results of laboratory and radiology test and other health-related information of patients are securely and instantly available to patients and doctors [2,3].

¹Faculty of Computer Applications, Ganpat University, Mehsana, India

The traditional health record system is ineffective as well as cumbersome because the medical records are documented on paper only [2]. By using the EHR system the data can be retrieved easily and efficiently, which is not possible in the traditional system [1]. The global monitoring of individual's health situations is restricted in the traditional system, whereas the EHR system shares patient's health data with other health systems with an objective to accumulate health-related data from various sources at different time [4]. The information sharing among providers using the EHR enhances the care to be taken to patients and decreases medical errors [1].

The objective of EHR is to provide an efficient, secure and reliable way to store, access and process all the medical information regarding patient's health. The EHR improves quality in health-care system and enables one to share data electronically. It also helps one to take action for the treatment of patients and medical practice [5].

To gain patient's trust, the EHR system should be made successful. If the privacy of health information is not kept by providers, then patients would lose his/her trust on the EHR system. It can stop patients from disclosing important information regarding health and insist to refuse the use of the EHR system [2].

3.1.2 *Workflow of traditional medical care system*

The workflow of the traditional medical care system is shown in Figure 3.1 and steps show about how the traditional medical care system works.

1. The patient calls a hospital and takes an appointment.
2. The day before the appointment, patient's files are drawn from the health record filling system and organized for next day's appointment.
3. The patient reaches medical office on appointment day and requests to verify his demographic and insurance information. Then the patient is given the



Figure 3.1 *Workflow of the traditional medical care system*

medical history form to fill up. In filling up the details such as medical history, purpose of visit, new allergies, changes in medicine are to be furnished.

4. After that, the patient moves to a room to get examined. Then a nurse would ask the patient about his/her problems, symptoms etc. in his/her version.

After reviewing the form, which is filled up by patients, the nurse measures the weight, height and necessary signs of the patient. All these things are verified and written in the form and are kept for future use.

5. After that, the doctor comes into room and examines the symptoms and asks about reasons of visit. Then the doctor examines and observes those as reported by the patient. Now the trained nurse examines the patient as per findings, and the doctor concludes about the cause behind patient's illness and which tests are necessary for further diagnosis. Then, the doctor prescribes medicines and test. The doctor also recommends about the next visit of the patient. For each element a chart note is made.
6. The prescription is given to patients or refers to a pharmacy. A note is left on patient's chart using a diagnose code and a billing code; then the doctor leaves the room.
7. If any lab work is required, the nurse takes samples and sends it to lab.
8. The doctor makes a note taking information from patient's form, nurse's form, treatment and plans on the basis of medical knowledge.
9. After getting the patient dressed up, he/she will be guided to reach the checkout area. Instructions for medicine and care are given. If any other tests or X-ray are to be performed in other facilities, office staff can schedule it on behalf of the patient. If it is necessary to take any follow-up, then the next appointment is scheduled.
10. Notes are given to the doctor for proper dictation and recorded permanently. Then these notes are reviewed through the billing person to check codes for billing.
11. If any lab testing is performed, X-ray or any other diagnostic reports are sent by mails or fax or paper to the patient. Then the office person fills up the chart of patients and sends it to the doctor for a review. Then review is done by the doctor and the chart is re-filled.
12. At last the paper chart is filled again with lab reports after doctor's review.

3.1.3 Workflow of electronic health record system

The workflow of electronic health record system is shown in Figure 3.2 and steps show about how EHR system works.

1. The patient calls the hospital and takes an appointment. In an alternative way, the patient visits the hospital portal and requests for an appointment and gets a confirmation through internet.
2. The day before the appointment, the computer system electronically verifies patient's insurance policy and schedules an appointment for the next day.
3. The patient reaches the medical office on the appointment day and asks to verify his demographic information for correctness.
4. A nurse or receptionist gives the medical history form to fill up in a computer. The patient fills up the details, such as medical history, purpose of visit, new



Figure 3.2 Workflow of electronic health record system

allergies, and changes in medicine. Some hospital portals allow patients to fill these details using internet before arriving.

5. When the patient fills this questionnaire, the computer system notifies the nurse about the completion of filling up the form and preparedness for examining. The nurse measures the weight and height and records information in the EHR system. She uses electronic devices to measure temperature, pulse, blood pressure, records and transfers into the HER.
6. The nurse examines the information of symptoms and history entered by the patient. If necessary, she edits the records for further clarification. Then the doctor examines the patient and discusses about visit and symptoms that are already in the chart.
7. The doctor physically and psychologically examines the patient, and the reports are used for the selection of template in the EHR for easy storing and retrieving the information from the EHR. The EHR also shows the list of problems that are not resolved in the previous visit. The doctor examines additional reports if necessary, notes the changes whether it is positive or negative. After assessing the patient health condition and taking feedback from the nurse, the doctor concludes his decision about diagnosis and decides whether further tests would be required or not.
8. Then, the doctor gives prescription about medicine, test and for treatment. The EHR system provides materials for counseling and education, decision support, quality screening report and provides research on patient's condition on

evidence observed. For ordering the medicine, the doctor writes prescriptions electronically. Then in the EHR, comparison is done on the basis of current medicines and allergy records of the patient. The doctor counsels if any problems arise. In addition, the comparison of prescription with formulary of drugs covered in insurance plan is done, and, if necessary, other medicines are recommended. Then the prescription is directly transferred to the pharmacy. The EHR suggests the proper code for managing bill. This code is confirmed by the doctor and the bill will automatically be transferred to the billing system. The doctor signs on the exam note electronically and concludes the visit.

9. If any lab work is left, then the nurse will take specimen and send it to lab electronically.
10. The doctor can provide more time for counseling or educating the patient because of the EHR system. By using the system, the doctor shows some display of body parts and educates the patient and prints the copies of the body parts for the patient to take those home.

The patient will be guided for the checkout area. Then education materials, instructions for medicines and care and the copy of the exam note will be given. Using hospital's secure website, the patient can access his/her health records.

11. If any other tests or X-ray are done in other facilities, then the office staff can schedule it on behalf of the patient. If it is necessary to take a follow-up, then the next appointment should be scheduled.
12. The result of the lab test or radiology reports are forward to the doctor electronically, which is reviewed on a screen and recorded to the EHR.

3.1.4 Advantages of the EHR system

The following advantages are categorized after implementing the EHR system in an organization.

1. According to the patient
 - (i) Manages quickly their records.
 - (ii) Decreases time of telephone calling and messaging for appointment and medicine refills.
 - (iii) Patients get accurate and timely information regarding care.
 - (iv) Decreases duplicate treatment and test.
2. According to the clinician
 - (i) Manages quickly telephone and messaging for appointments and medicine refills and reduces tedious and repetitive task.
 - (ii) Increases intracommunications between offices.
 - (iii) Remotely takes access to the information of patients.
 - (iv) Decreases chart pulls.
 - (v) Enables efficient and quality-assured clinical practice.
 - (vi) Improvement in billing and financial system.
 - (vii) Reduction in paper errors and cost.
 - (viii) Increases clear formulary compliance and prescription and decreases pharmacy call back.

3. According to the society

- (i) Increases the observation of public health and disease investigation.
- (ii) Supports in gathering complete statistic details for framing public health policy.
- (iii) Efficiency should be brought in total expenditure of health.

3.2 Scratch for privacy and security concern

The security and privacy are major concerns for increasing patient's trust and information integration. The health information of persons should be secure and private within individuals and providers for getting healthier results as well as healthier persons. The patient cannot disclose his/her health information, if he/she finds risk on accuracy and confidentiality in the EHR because they have less trust on EHRs and health information exchanges. The security and privacy of health records play a vital role because holding of health information of patients could create life-threatening significances.

3.2.1 *Background of health information privacy and security*

Privacy is the leading principal within a patient and a doctor for actual distribution regarding health care. To avert remedy interaction, the patients should share their information to doctors for diagnosing right disease and take corrective actions for treatment. In some situations, patients do not want to share information in cases such as HIV information or psychiatric disorders because it may lead to social scar and prejudice [6]. In addition to medical information of patients, the patient's identification is also collected, that is, personal information, past medical judgment, nature of treatment from previous doctors, digital representation of medical images, history of drugs, habits of diet, heredity information, psychological summaries, sexual liking, history of employment and income, mental and personal state amongst others [7].

3.2.2 *Privacy and confidentiality*

Privacy means the right of persons who keep information within themselves, without disclosing to others [8]. The claim of a person should be considered without any interferences from other persons, government or any organizations [9].

The information that is shared as consequences of medical relationship should be protected because it is considered confidential [10]. The data such as laboratory test results, diagnoses results, identification information and progress reports can be stored in different forms such as text, images, and video. The information regarding identity of patient cannot be disclosed in case patients have prostate cancer [11].

The information of patients should be released as per law or after permission is taken from patients, although the doctor cannot get patient's information without any permission. The doctor can share patient's information for the sake of treatment, administrator or payment purpose. Patients also have rights to view, copy or change information regarding their health.

Confidentiality makes sure that only an authorized person can access the information. It also contains the process of access about the limitation of users for getting information. From the doctor side, the administrator first identifies the number of users, the access level of information based on role privileges for each user and assigns a username and a password. For example, the receptionist and the nurse have different tasks and responsibilities, so they cannot access the same information.

3.2.3 Security

Since the emerging of EHR, security has been the major concern for health information, because nowadays the use of smart phones and mobile devices has increased. Usually the transaction of information within doctors, patients and federal agencies is kept secret, still the theft in medical identity has been increasing.

The patients cannot frank with the doctor, if his/her trust is broken. To sustain the trust of patient's medical record, information should be protected. The medical staff should be aware of security standards to secure patient's data and the data within medical practices.

As per a survey, 73% doctors write messages or text to other doctors about their work [12]. During the transmission of text, security is a major concern. There is no other way of controlling communications that are intercepted by opponents on data and images that are supposed to be transferred and shared; level of details and devices that are used for transferring are secure; and text are encrypted. The mobile devices are used for individual use and it cannot design for centralized management [13]. The computer terminals are hardly lost; however, mobiles can be damaged, misplaced or stolen easily. That is why it is important to use encrypted mobile devices for transmitting confidential information.

To avoid potential threats such as alteration, hacking or damage of information by external or internal users, education programs should be organized and security standards should be available to all users. The antivirus s/w, firewalls, intrusion detection s/w can be used as security standard to protect data. In addition, full security programs are installed in systems to maintain integrity of information and audit trails should be operational to monitor the persons who have access to patient's data.

Audit trails are used for racking all the activities of the system, time and date for every entry, persons' identities who view details, with respective time, and managing logs of all alterations in records [14]. An admin person can get the details of printed reports, screen shots and track the computer location from the received request. The audit trails can be used for the prevention of violators but cannot prevent from unauthorized access or information disclosure.

3.2.4 Problems arise in security and privacy

It is mandatory to give assurances to patient's privacy against the risk associated with the EHR. The following issues of security should be properly considered at the time of using the EHR system.

1. *Verification of users:* Only authorized users have right to access health records. Different authentication systems such as token- and biometric-based

authentication systems should give assurance to an authorized access to records [15].

2. *Integrity and confidentiality*: It is a concern for the reliability and integrity of computer and network systems as well as the accuracy and reliability of health records. The modification of data and damage of health records may be made by hacking of EHR [16].
3. *Access control*: It is a vital issue for security to share computer environments in which health records are stored in a database. The rights of users' roles are different based on the nature of organization and system. Therefore, it is necessary to control rights of users for accessing and refusing the use of resources. It is hard to identify a user who is accessing the network in non-secure remote connection [17]. The EHR system must have some features for security such as role-wise access of system, audit trails and authentication system. There are certain issues of privacy regarding genetic test. Persons fear for loss of life insurance and loss of employment. That is why performing genetic test is rejected, as it harms patients, doctors and researchers [17].
4. *Data control*: It is also important to give rights to access patient's data. Allowing users to access to the respective data, allocation of authority on data and transparency should be provided to owners of health records [18].
5. *Data security policies*: The security should be necessary because many organizations are involved in medical diagnosis. The organization has to decide function limitations in advance. The organization has to implement strict rules and initiate processes for preventing loss or theft of portable devices and physical media. EHR system has to regularly develop some functionality to handle blockage in access of labs result and some notes, manage security with increasing the level of security, track of visioning, encrypt entries and so on [19].
6. *Profiles of users*: Many entities such as doctors, patients, medical organizations and pharmacists are involved in health-care system. Still issues are there where, as per role of users, variations in security levels and functionality should be there [19]. It is difficult to identify patients within different units, because there is large incompatibility in health-care system. There is no system that matches records that create interoperability within units [20].
7. *Misuse of health record*: The privacy is not concerned when offering free storage space, and most of the websites offer EHR free space for storage. In that case, the misuse of data happens because of selling it to other enterprises or by uploading advertisements on that page by the patient itself [21]. The security of medical records is a challenging task in multispecialist situations. The system should be capable of separating records regarding the treatment of physique exploitation, because in this type of treatment multiple types of document and specialists are involved [21].

3.3 The HIPAA rules and patient's rights for health care

The Health Insurance Portability and Accountability Act (HIPAA) rules give assurances to tolerant wellbeing data held by Covered Entities (CEs) and Business

Associates (BAs) and give patients various privileges for that data. This suite of directions incorporates the following:

- *The privacy rule* ensures security of data.
- *The security rule* ensures models of e-Health Data.
- *The breach notification rule* requires giving warnings after a break of uncontrolled and confined Health data.

Entities must conform to the act for privacy, security and breach notification rules. Associates must agree to the act for security rule and breach notification rule and certain arrangements of the act privacy rule.

The privacy rule builds up a general standard for wellbeing data protection. It addresses the exploitation and exposure of people's health information and also morality to understand and control how their wellbeing data is utilized and shared, including rights to look at and acquire a duplicate copy of their wellbeing records in addition to asking for amendments.

Regardless of whether quiet wellbeing data is available online, in an EHR, on paper, or in other media, suppliers have obligations regarding defending the data by meeting the necessities of the rules.

This part gives an extensive outline of the health act protection and security necessities, associated, in any frame or media, regardless of being electronic, paper or oral. The act calls this data "ensured wellbeing data." Individually recognizable wellbeing data is the one, including statistic data that identifies patients' all conditions and medical records.

Similarly, independently recognizable wellbeing data distinguishes individuals or there is a sensible premise to trust it that tends to be utilized to recognize persons.

The act does not matter to exclusively recognizable wellbeing data in your training's business records or in records secured by the FERPA, as revised.

Entities and associates must consent to the act rules. Entities are medicinal services suppliers, welfare designs, medicinal services providers.

Associates are an individual or substance, other than a workforce part. BA capacities or exercises incorporate cases preparing, information examination, quality affirmation, certain patient security exercises, use survey and charging.

3.3.1 The HIPAA privacy rule

The privacy rule ensures the norms for safeguard of health data. It addresses the utilization and disclosure of welfare information of the people and also gages for people's security rights to comprehend and control how their wellbeing data is utilized and shared, including rights to look at and acquire duplicate wellbeing records and additionally to ask for redresses.

The act restricts employees' revelation of patient's history: Some of the questions insist to limit privacy rule like how to use patients' information, how to get patients' permission for disclosing the information for psychotherapy, upholding activities and licensing. State administration also provides privacy laws for protection.

3.3.2 *The HIPAA security rule*

The Health Act Security Rule ensures national arrangement of least security models for ensuring all e-patients' fitness records as well as medical history.

These act shields can enable wellbeing to mind suppliers who maintain a strategic distance from a portion of the regular security holes that could prompt digital assault interruptions and information misfortune. Shields can secure the general population, data, innovation and offices that social insurance suppliers rely upon to complete their essential mission: thinking about their patients.

The act has a few kinds of protections and necessities that you should apply: decision-making protection, corporal protection, trustworthy principles, and policies and procedures.

3.3.3 *The breach notification rule*

A breach is, by and large, an impermissible use or disclosure under the privacy rule that bargains the security or protection of Protected Health Information (PHI). An impermissible use or revelation of unbound people history is attempted to be a rupture except if the entities or associates illustrate that people's record has been compromised. When a breach of unbound information happens, the act requires your training to inform influenced people, the secretary of system, and, now and again, the media [22].

The act insists entities to tell people and the secretary of system of the misfortune, burglary or certain other impermissible utilizations or revelations of unbound history of data. Specifically, human service suppliers should speedily advise the secretary of Health and Human Services (HHS) if there is any rupture of unbound PHI that influences at least 500 people, and they should inform the media if the breach influences in an excess of 500 inhabitants of a state or purview. In the event that a breach influences less than 500 people, the CE should advise the secretary and influence people. Reports of ruptures influence less than 500 people because the secretary restricts it within 60 days after the end of the date-book year in which the breaches happened [22].

- Huge ruptures are explored by Optical Character Recognition (OCR), and punishments might be forced for inability to conform to the HIPAA rules. Breaches that influence at least 500 patients are freely provided details regarding the OCR website.
- Comparative breach warning arrangements are actualized and authorized by the FTC to history of patient engineers and their outsider specialist organizations.

On the off chance that you can show through a hazard evaluation that there is a low likelihood that for the utilization or divulgence traded off unbound PHI, at that point, rupture warning is not essential. (It would be ideal if you take a note of that this breach-related hazard evaluation is not quite the same as the intermittent security chance examination required by the security rule.)

In addition to the event that you scramble your information as per the OCR direction with respect to rendering information unusable, muddled or incomprehensible, you may refrain from revealing what might somehow or another have been a reportable break. Encryption relies upon the encryption key being kept

profoundly classified, so it should not be stored with the information or kept in an area that would bargain it.

3.4 Hazard capacity method for breaches

When you speculate that a break of unbound history has happened, first direct a hazard evaluation so as to look at the probability that the PHI has been endangered. For you to show that a rupture has not bargained PHI, your training must direct the hazard appraisal in compliance with common decency and by altogether evaluating in any affair the four required components are recorded beneath.

- The scenery and degree of the history of patients are associated with exploitation or exposure, including the sorts of identifiers and the probability that PHI could be redistinguished. As noted above, if your training has a break of encoded information and in the event that you had followed standard encryption particulars, it would not be viewed as a rupture of unsecured information, and you would not need to report it.
- Unapproved individuals who use the history of patients or to whom the divulgence was made (e.g., a sibling or a writer).
- The probability that any PHI is really obtained or seen (e.g., a review trail would give bits of knowledge).
- The degree of hazards to the history of people has been moderated. By playing out this appraisal, anyone can address any component independently and afterward dissect the consolidated four components to decide the general likelihood that the history of patient has been endangered. The completion of OCR must be sensible. The degree of exhibiting an utilization or revelation of unbound historical records of patients did not establish a rupture. In the event, this evaluation demonstrates that there is
 - Low likelihood of bargained PHI, at that point the utilization or divulgence is not viewed as a rupture and no warning is important.
 - Likelihood of bargained PHI, break notice is required.

3.4.1 Revealing breaches

In the event that you decide not to direct the hazard evaluation, or if, in the wake of playing out the hazard appraisal sketched out above, you confirm that break warning is required. There are three kinds of notices to be made to people, to the secretary of HHS and, at times, to the media. The quantity of people that are influenced by the break of unbound health records decides your warning prerequisites.

3.4.2 Examination and enforcement of potential ACT violations

OCR starts an endless supply of complaints, rupture reports, data given by different offices and the media. The ACT Enforcement Rule gives diverse punishments to every one of four dimensions of culpability [22,23]:

- Contravention that the element did not think about and would not have thought about by practicing sensible perseverance.

- Contravention because of “sensible reason.”
- Contravention because of “tenacious disregard” that are remedied inside 30 days.
- Contravention because of “obstinate disregard” that are not adjusted within 30 days.

3.4.3 *Understanding patients’ health information rights*

The act addresses the utilization and revelation of people’s protected health records by associations subject to the privacy rule. The rule likewise addresses models for people’s protection rights with the goal that patients can comprehend and control how their wellbeing data is utilized and revealed. The OCR clarifies these rights and different prerequisites which are more complete on its site, incorporating into its summary of the act [22].

As a human service supplier, you have obligations to patients under the act of privacy, incorporating by giving them a notice of privacy practices and reacting to their solicitations for access, changes, bookkeeping of exposures, limitations on utilizations and revelations of their wellbeing data, and secret interchanges.

EHR Incentive Programs include new rights for patients who need their social insurance suppliers to transmit their electronic histories to themselves or different parental figures.

NPP: Entities furnish your patients with a notice of your protection rehearses. Your notice must contain certain components, including

- Depiction of how your training may utilize or uncover people health records.
- Determination of people’s rights, including the privilege to whine to the US Branch of HHS and to your training in the event that they trust their security rights have been damaged.

Quiet access to information: Patients have privileges to examine and get a duplicate copy of their history in an assigned history, which incorporates data about them in the therapeutic and charging records. (Assigned record sets are clarified toward the end of this section.) Entities should concede or deny the demand for access within 30 days of the receipt of demand. In the event that the wellbeing data is held in electronic arrangement and the patient’s solicitations to get it in an explicit electronic organization, an entity should give it in the e-history asked for by the patient in the event that it is promptly producible. On the off chance that the configuration is not accessible, the entity should give the wellbeing data in an electronic organization consented by the patient and entities.

Altering patient information: Under the act, patients have the privilege to ask for that their training changes their PHI in an assigned record set. For the most part, an entity should respect the demand except if it has confirmed that the data is exact and complete. The CE should follow up on a person’s demand for a change within 60 days after the receipt of the demand. To acknowledge a revision asked for, the training must make a suitable change by distinguishing the records in the assigned record set that are influenced by the correction and giving a connection to the area of the alteration. In the event that you decline the demand, extra prerequisites, including the patient’s entitlement to document an announcement of difference that stays with the wellbeing record, apply.

Bookkeeping of disclosures: People have a privilege to get a bookkeeping of disclosures 43 of their PHI made by your training to an individual or association outside of your training. A bookkeeping of revelations is a posting of the

- names of the individual or substance to whom the history was unveiled,
- date on which the history was revealed,
- depiction of the history unveiled,
- reason for the revelation.

The privilege to a bookkeeping is constrained, as the rule does not expect you to incorporate revelations made for treatment, installment, health-care tasks and a few different purposes and circumstances.

Rights to restrict information: People have the privilege to ask for that your training confine certain

- Utilizations and revelations of people medical history for cure, installment and human services activities.
- Revelations to people engaged in the person's human services or installment for medicinal services.
- Exposures to advice relatives or others about the person's general condition, area or demise.

Ideal to confidential communications: Model training must suit sensible demands by your patients to get correspondences from you by the methods or at the areas they indicate. For instance, they may ask for that arrangement updates be left on their work voice message as opposed to home telephone phone message [24,25].

3.5 Generalize E-health-care models

To enhance the nature of human service conveyance, patient's information could be shared over an assortment of clients, which may prompt protection divulgence. Along these lines, e-health frameworks should be ensured through advantageous security models to guarantee legitimate access controls. Truth be told, encryption is the customary arrangement utilized. In spite of the fact that it gives a basic access control, it is not material for complex record keeping frameworks that require different access prerequisites. That is, keeping the e-health information anchored is a major test because of two fundamental reasons: the critical computational overhead when encryption systems were utilized, and the affectability of individual therapeutic data from changing when adjustment methods are utilized. In this segment, a definite portrayal of a number of security models, alongside their comparing levels, are exhibited [37–39].

1. *Safety measures models for data gathering level:* Many models are available to make a control over the access to data for medical services-based applications. In addition the proposed way to deal with a planned lightweight security display model is available—one model for adaptive access control to medical service providers, the other for preconveyance patterns that refer to three-level

security, one more model based on biometric security structure and the one most administrative model based on sensor to provide security [26–31].

2. *Safety measures models for data communication level:* Many models are based on this level to protect the structure of information verification for transmission and also apply encryption procedure. The other secure plan boosts up with noteworthy people personal and medical access information as per privileges. One more model was available for working at this level using the mechanism of cloud- and sensor-based system. Then another model was proposed that works with Secure Socket Layer (SSL) and really light weight security system. One more model is available in which the proposed model comprises eight center segments such as subject qualities, objects, protest characteristics, rights, approvals, commitments and conditions. Although approvals, commitments and conditions are parts of use, control choices use to decide if a subject is permitted to get to a protest [42–50].

3.6 Conclusions and current scope of research

Innovation is empowering medicinal wellbeing records to be put in the EPRs, and making them accessible to the peoples or patients via net connectivity. Moreover, progresses in the zone of sensor systems are making the possibility of remote tolerant checking a reality. The defense and safety measure issues are come out by integrating the original novelty into the routine healing service framework. People health histories ought to be kept safely in healing sector and supplier servers with a goal that medical practitioner can give suitable medications. To guarantee secure capacity and access the board, in this chapter, we contend the security assaults in social insurance framework alongside the proposed security models that plan to anticipate such assaults. In particular, dangers were sorted into three kinds relying upon its developed dimension of the medicinal services framework, for example, at information gathering level, at transmission level and at capacity level. These assaults may cause a few dangers, for example, changing data, dropping some critical information, intruding on correspondence or sending additional signs to obstruct the base station and expanding organizing traffic [36,40,41].

From that point onward, we quickly have examined a novel setting mindful access control security demonstrating which underpins the security basics of social insurance frameworks and giving fine-grained access to control. The model comprises numerous modules, every one of which is accountable for taking an alternate sort of errand. This measured plan goes for basic and productive access control choice relying upon the patient's circumstance and the requester's relegated jobs.

References

- [1] Handel DA, and Hackman JL, Implementing electronic health records in the emergency department. *The Journal of Emergency Medicine*, 2010, 38: p. 257–263.

- [2] Acharya S, Coats B, Saluja A, and Fuller D, Secure electronic health record exchange: achieving the meaningful use objectives. *International Conference on System Sciences*, 2013, 46: p. 1–10.
- [3] Rosenthal DI, Instant replay. *Healthcare*, 2013, 1: p. 52–54.
- [4] Nocco L, and Peigné V, An empirical study of healthcare providers and patient's perceptions of electronic health records. *Computers in Biology and Medicine*, 2014, 59: p. 194–201.
- [5] Tang PC, Ash JS, and Bates DW, Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association*, 2006, 13: p. 121–126.
- [6] Applebaum PS, Privacy in psychiatric treatment: threats and response. *American Journal of Psychiatry*, 2002, 159: p. 1809–1818.
- [7] Mercuri RT, The HIPPA-potamus in health care data security. *Communications of the ACM*, 2004, 47: p. 1–7.
- [8] Warren SD, and Brandeis LD, The right to privacy. *Harvard Law Review*, 1890, 4: p. 193.
- [9] Rognehaugh R, *The Health Information Technology Dictionary*. Gaithersburg, MD, USA: Aspen; 1999:125.
- [10] Rinehart-Thompson LA, and Harman LB, Privacy and confidentiality. In: Harman LB, ed. *Ethical Challenges in the Management of Health Information*. 2nd ed. Sudbury, MA, USA: Jones and Bartlett; 2006:53.
- [11] Rinehart-Thompson LA, and Harman LB, Privacy and confidentiality. In: Harman LB, ed. *Ethical Challenges in the Management of Health Information*. 2nd ed. Sudbury, MA, USA: Jones and Bartlett; 2006:54.
- [12] Greene AH, HHS steps up HIPAA audits: now is the time to review security policies and procedures. *Journal of American Health Information Management Association*, 2011, 82(10): p. 58–59. <http://www.ahimajournal-digital.com/ahimajournal/201110?pg=61#pg61>. Accessed August 10, 2012.
- [13] AHIMA. "Mobile Device Security (Updated) - Retired." *Journal of AHIMA*, (April 2012), 83(4): 50–55. [Online: https://bok.ahima.org/doc?oid=105345#.XVpmTUDS_IU]
- [14] American Health Information Management Association, Copy Functionality Toolkit; 2008:4. http://library.ahima.org/29%3Cand%3E%28xPublishSite%3Csubstring%3E%60BoK%60%29&SortField=xPubDate&SortOrder=Desc&dDocName=bok1_042564&HighlightType=PdfHighlight. Accessed August 10, 2012.
- [15] Yang Y, Han X, Bao F, and Deng RH, A smart-card-enabled privacy preserving E-prescription system. *IEEE Transactions on Information Technology in Biomedicine*, 2004, 8(1), 47–58.
- [16] Katzenbeisser S, and Petkovic M, Privacy preserving recommendation systems for consumer healthcare services. in *IEEE 3rd International Conference on Availability, Reliability, and Security*. 2008.
- [17] Al-hamdani W, *Cryptography Based Access Control in Healthcare Web Systems*. Kennesaw, GA, USA: ACM; October 2010. 9781-60558-661-8/10/10 infosecCD'10.

- [18] Huda MDN, and Sonehra Y, A privacy management architecture for patient-controlled personal health record system. *Journal of Engineering Science and Technology*, 2009, 4(2), p. 154–170.
- [19] Vucetic M, Uzelac A, and Gligoric N, E-Health Transformation Model in Serbia: Design, Architecture and Developing. In *2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. 2011, p. 566–573. IEEE.
- [20] Ateniese G, and de Medeiros B, Anonymous e-prescriptions. In *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, 2002, p. 19–31. ACM.
- [21] Riedl B, Grascher V, Fenz S, and Neubauer T, Pseudonymization for improving the privacy in e-health applications. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 255–255). IEEE.
- [22] Guide to Privacy and Security of Electronic Health Information. (n.d.). Retrieved from <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>.
- [23] Mare S, Sorber J, Shin M, Cornelius C, and Kotz D, Adapt-lite: Privacy-aware, secure, and efficient mhealth sensing. In *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society (WPES'11)*. 2011. ACM, New York, NY, USA, 137–142.
- [24] Jin W, Zhongqi Z, Kaijie X, Yue Y, and Ping G, A research on security and privacy issues for patient related data in medical organization system. *International Journal of Security and Its Applications*, 2013, 7(4): p. 287–298.
- [25] Zhang K, Yang K, Liang X, Su Z, Shen X, and Luo HH, “Security and privacy for mobile healthcare networks: From a quality of protection perspective,” in *IEEE Wireless Communications*, 2015, 22(4): p. 104–112.
- [26] Garcia-Morchon O, and Wehrle K, Efficient and context-aware access control for pervasive medical sensor networks. in *Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2010 8th IEEE International Conference on. 2010. IEEE.
- [27] Amini S, Verhoeven R, Lukkien J, and Chen S, “Toward a security model for a body sensor platform,” *2011 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, 2011, p. 143–144.
- [28] Maw HA, Xiao H, and Christianson B, An adaptive access control model for medical data in wireless sensor networks. in *e-Health Networking, Applications & Services (Healthcom)*, 2013 IEEE 15th International Conference on. 2013. IEEE.
- [29] Linciya T, and Anandkumar K, Enhanced three tier security architecture for WSN against mobile sink replication attacks using mutual authentication scheme. *International Journal of Wireless & Mobile Networks*, 2013, 5(2): p. 81.
- [30] Rasheed A, and Mahapatra RN, The three-tier security scheme in wireless sensor networks with mobile sinks. *IEEE Transactions on Parallel and Distributed Systems*, 2012, 23(5): p. 958–965.

- [31] Ramli SN, Ahmad R, Abdollah MF, and Dutkiewicz E, "A biometric-based security for data authentication in Wireless Body Area Network (WBAN)," 2013 15th International Conference on Advanced Communications Technology (ICACT), PyeongChang, 2013, p. 998–1001.
- [32] Boonyarattaphan A, Bai Y, and Chung S, A security framework for e-health service authentication and e-health data transmission. in Communications and Information Technology, 2009 ISCIT 2009. 9th International Symposium on. 2009. IEEE.
- [33] Guan Z, Yang T, and Du X, Achieving secure and efficient data access control for cloud-integrated body sensor networks. *International Journal of Distributed Sensor Networks*, 2015, 2015: p. 142.
- [34] Simplicio MA, Iwaya LH, Barros BM, Carvalho TCMB, and Näslund M, "SecourHealth: A delay-tolerant security framework for mobile health data collection," in *IEEE Journal of Biomedical and Health Informatics*, 2015, 19(2): p. 761–772.
- [35] Guo L, Zhang C, Sun J, and Fang Y, "PAAS: A privacy-preserving attribute-based authentication system for eHealth networks," 2012 IEEE 32nd International Conference on Distributed Computing Systems, Macau, 2012, p. 224–233.
- [36] Sun J, *Security and Privacy for Mobile Healthcare (m-Health) Systems*. Amsterdam, The Netherlands: Elsevier; 2011.
- [37] Barua M, Liang X, Lu R, and Shen X, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, 2011, p. 970–975.
- [38] Fernández-Alemán JL, Senor IC, Lozoya PÁ, and Toval A, Security and privacy in electronic health records: a systematic literature review. *Journal of Biomedical Informatics*, 2013, 46(3): p. 541–562.
- [39] Shinde SS, and Patil D, Review on security and privacy for mobile healthcare networks: from a quality of protection perspective international. *Journal of Engineering Research-Online Peer Reviewed International Journal*, 2015, 3(6): p. 1–24.
- [40] Habib K, Torjusen A, and Leister W, Security analysis of a patient monitoring system for the Internet of Things in ehealth. in *Proceedings of the International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED'15)*. 2015.
- [41] Kumar MR, Fathima MD, and Mahendran M, Personal health data storage protection on cloud using MA-ABE. *International Journal of Computer Applications*, 2013, 75(8): 11–16.
- [42] Kumari A, Tanwar S, Tyagi S, and Kumar N, Fog computing for healthcare 4.0 environment: opportunities and challenges. *Computers & Electrical Engineering*, 2018, 72: p. 1–13.
- [43] Vora J, Tanwar S, Verma JP, *et al.*, BHEEM: a blockchain-based framework for securing electronic health records. in *IEEE Global Communications*

- Conference (IEEE GLOBECOM-2018), Abu Dhabi, UAE. 09–13 December 2018, pp. 1–6.
- [44] Vora J, Devmurari P, Tanwar S, Tyagi S, Kumar N, and Obaidat MS, Blind signatures based secured E-healthcare system. in International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018), Colmar, France. 11–13 July 2018, pp. 177–181.
- [45] Hathaliya J, Tanwar S, Tyagi S, and Kumar N, Securing electronics healthcare records in healthcare 4.0: a biometric-based approach. *Computers & Electrical Engineering*, 2019, 76: p. 398–410.
- [46] Vora J, Tanwar S, Tyagi S, Kumar N, and Rodrigues JPC, FAAL: fog computing-based patient monitoring system for ambient assisted living. in IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom-2017), Dalian University, Dalian, China. 12–15 October 2017, pp. 1–6.
- [47] Vora J, Italiya P, Tanwar S, *et al.*, Ensuring privacy and security in E-health records. in International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018), Colmar, France. 11–13 July 2018, pp. 192–196.
- [48] Tanwar S, Thakkar K, Thakor R, and Singh PK, M-tesla-based security assessment in wireless sensor network. in International Conference on Computational Intelligence and Data Science (ICCIDS 2018), NorthCap University, Gurugram. 07–08 April 2018.
- [49] Tanwar S, Obaidat MS, Tyagi S, and Kumar N. Online signature-based biometric recognition. In: Obaidat M, Traore I, Woungang I. (Eds.), *Biometric-Based Physical and Cybersecurity Systems* (pp. 255–285). Springer, 2019.
- [50] Tanwar S, Tyagi S, Kumar N, and Obaidat MS, Ethical, legal, and social implications of biometric technologies. In: Obaidat M, Traore I, and Woungang I. (Eds.), *Biometric-Based Physical and Cybersecurity Systems* (pp. 535–568). Springer, 2019.
- [51] Gartee RW, *Electronic Health Records: Understanding and Using Computerized Medical Records*. Upper Saddle River, NJ: Prentice-Hall, Inc.; 2006.

Chapter 4

Identity and access management systems

Darpan Anand¹ and Vineeta Khemchandani²

4.1 Introduction

Identity and access management (IAM) in a computer system includes a security framework, tools, and technologies to control access to critical information resources to legitimate users in the right context. IAM is even more challenging for healthcare organization as they are responsible for the protection of users identities and valuable medical records. Health care organizations are more prone to attacks than financial institutions. Data breaches in e-healthcare can lead to identifying theft, billing, and insurance frauds. To prevent such breaches IAM for health care must be even more secure and scalable to meet current challenges. IAM cannot be explained without learning the concept of identification.

Identification is an important process of any information communication technology (ICT)-based system where verification of a legitimate user is required. It is also important to link and further access the stored data, modules, and services with an entity. In the e-health care system, there is a requirement to identify the patient and according to it, the history will be accessed for further assessment by health experts. Therefore, it is an important and crucial process for the health services and government health management system. The important role to secure information interchange can be done through provide access only to the legitimate users, this functionality is called as accessibility. This is also useful to provide protection from the reveal of crucial information to the illegitimate firms/user. Generally, there are three entities involved in identification as Organization, Process, and Technology; and through the combination of these, the life-cycle of identification takes place as illustrated in Figure 4.1.

One of the application of identification is to provide access to the user as per authorization. The management of identity and access is access management. The access management is the process of secure evaluation of the legitimate entities to

¹Department of C.S.E.-UIE, Chandigarh University, Chandigarh, India

²Department of C.S.E., J.S.S. Academy of Technical Education, Noida, India

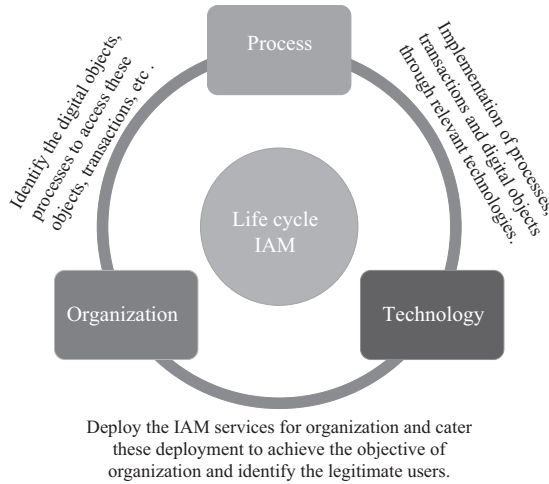


Figure 4.1 Life-cycle of identification

access particular computing resources or digital objects. Generally, these resources and objects include these services, receptacle information like remote files, web resources, etc. The access management works over an existing security context and also controls various interconnected resources of the system. The access management policies are implemented in the forms of rules which can be static as permissions, access rights, roles, or dynamically deduced rules and rights. The primary focus of the access management is on authentication then authorization which evaluates the limits of accessibility to digital resources. This chapter discusses concepts and various research-oriented IAM techniques for growing connected healthcare system.

4.2 ISO standards for security

Every organization does its best to make its system secure and effective. The security of products and policies are assessed and evaluated by a standard that are OSI security architecture suggested by a United Nations-sponsored agency The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T). This standard is responsible to suggest some systematic methods for defining the security requirements and security goals. Further, this standard evaluates the approaches to satisfy these security requirements and security goals. OSI security architecture concentrates on three entities, that is, attack, mechanism, and service. This architecture can be applied for every software system for all security requirements as of confidentiality, integrity, availability, etc. [1].

OSI security architecture

The OSI security architecture is based on these three components as follows:

Security attack: This is an action which compromises the information security of an ICT system governed by an organization;

Security mechanism: This is a mechanism to detect, then prevent, and finally recover the system from various security attacks.

Security service: These services are processing or communication of information in the system, responsible to counter security attacks using various security mechanisms.

Security analysis of any ICT-based system is required on the basis of security requirements of the associated organization. OSI security standards provide the security analysis of basic architecture for the security evaluation of such systems. But for detail security analysis, ISO gives its own security standards known as ISO/IEC 27001 standard [2].

4.2.1 ISO/IEC 27001 standard

ISO/IEC 27001 is the standards for security which published by ISO along with International Electrotechnical Commission (IEC). These standards are also known as “*Information technology Security techniques – Information security management systems Requirements*”. The objectives of these standards are to establish, implement, maintain, and security improvement of the existing software system to transform in a secure system through information security management system (ISMS). The ISMS is a systematic approach used to manage the crucial, critical, and sensitive information of the organization so that it may remain secure [3].

4.2.2 ISO/IEC 9798

The ISO also provides the detail standards for authentication process which is ISO/IEC 9798-1:2010. The ISO/IEC 9798 specifies a model for authentication which includes general constraints and requirements for authentication techniques like entity-authentication, etc. These authentication techniques are applied for verification of the legitimacy of an entity who requests to access the system through its identity credentials. Further, this standard also defines the guidelines for authentication algorithms, key management techniques, etc. [4]. ISO/IEC 9798 standard is classified into six parts based on different protocols and mechanisms as follows:

Classification of ISO/IEC 9798 standards

1. Part 1: General authentication techniques.
2. Part 2: Symmetric encryption algorithms-based authentication techniques.
3. Part 3: Digital signature techniques-based authentication techniques.

4. Part 4: Cryptographic check function–based authentication techniques.
5. Part 5: Zero-knowledge techniques–based authentication techniques.
6. Part 6: Manual data transfer–based authentication techniques.

4.3 **Authentication, authorization, and access management**

The process of authentication and authorization (A&A) is about to address the verification of the legitimacy of the user and then allow them to access the respective services. Usually, the process of authentication and authorization is being executed in a single system. To understand this process the following terms are very important. The overview of A&A is illustrated in Figure 4.2.

4.3.1 *Identification*

Definition 1: *The mechanism developed to the identification of a user reported to an automated information processing system is called as identification. In general, identification is processed by using the unique machine-readable names.*

The identification is a process, where the third entity will be sure about the identity of the entity which it claims. Suppose in case of college, every student has an ID-Card which is the token of identification of students. A student with ID-card is allowed to enter in the college and, if some student does not carry ID-card then he/she will not allow entering the college. Similarly, in the digital world, if some entity/process like to access service then, it should give a token/ticket/OTP, etc. to show its identity[5].

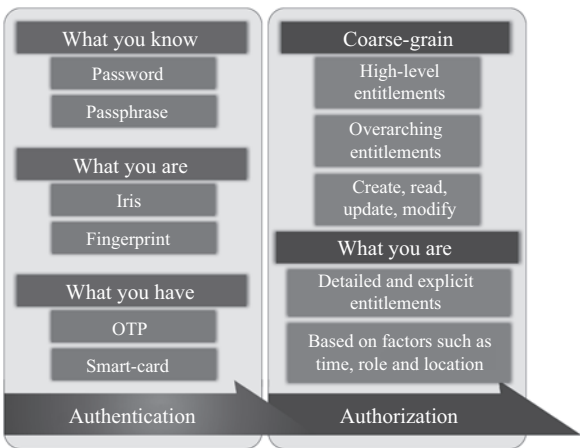


Figure 4.2 *Brief overview of authentication and authorization*

Types of identification techniques: There are basically three categories of identification as follows:

1. Entity-based identification
2. Architecture-based techniques
3. Process-based techniques

Entity-based identification: The entity-based authentication techniques are catered to let a party prove and verify the identity of another party. The entity involved in this mechanism may be a process, a person, a server, or a client. Two main entities are involved in this process are “*claimant*” and “*verifier*”. “*Claimant*” is an entity who claims its identity to be proved at “*verifier’s*” end. “*Verifier*” is an entity processes the requested identity to prove the legitimacy of the “*claimant*” at its ends. Entity-based authentication is a mechanism which authenticates the claimant for the entire duration of a session [6]. The categories of verification for entity-based identification are as follows:

Something known: In this category of entity-based authentication, the identity credentials are secret and only known to “*claimant*” that can be verified by the “*verifier*”.

Something possessed: In this category of entity-based authentication, the identity credentials of the “*claimant*” are processed to prove the legitimacy of it at the end of “*verifier*”.

Something inherent: In this category of entity-based authentication, the inherent characteristics and properties of the “*claimant*” are used to prove its identity.

Example: The simplest, oldest, and general method of entity-based authentication is the authentication technique based on a password. The identity of the “*claimant*” is proved by its password and it is only known to “*claimant*”.

Architecture-based identification: The computing of the computer system is depending on the various layers of the system where the identification of the “*claimant*” is also dependent on the system architecture. The user needs to be authenticated at the server when he/she wants to access the network services deployed at the same server. It is very tough to remember the various IDs and passwords by the user due to the increase in a number of services which are being deployed and available on remote servers. So, the multiserver architecture-based identification is required to verify the claimant. The system architecture is well defined for standard framework based applications like the web application but some applications are dependent on customized architecture. Therefore, system architecture-based identification techniques are required like Lightweight Directory Access Protocol (LDAP), Kerberos, multiserver protocols, etc.[7].

Process-based identification: This is the era of multiserver-based systems in which various transactions and communications will be taken place through distributed computing. The distributed computing needs various processes to control

Table 4.1 Examples of process authentication

Process authentication	Description
Kernel process ID and executable path	Executable may be modified or replaced when freely allowing access to the le system
SELinux Labels	Based on executable names, can be reused by malicious processes, subject to replay attack and policy misconguration
Hashes on les or code blocks	Have to recompute hashes at authentication at authentication
Developer-signed applications	May be forged or stolen, for example, Flame and Flashback malware; expensive to implement in kernel
Authenticated system calls	Only capable of verifying system call usage integrity, but not a general application authentication

the transactions like Secure Electronic Transactions (SET). The process should be identified and proved its legitimacy before completing any transaction. Therefore process-based identification techniques are useful [8]. Some important example of process-based identification is given in Table 4.1.

4.3.2 Authentication

Definition 2: *The action or mechanism of verifying the identity of a legitimate user or process.*

In a computer system, the actual person is not tied with his identity while the identity in computer systems belongs to service, process, or system through various factors like password, pass-phrase, one-time password (OTP), etc. To evaluate the verification of an entity, two basic processes are required to execute as registration and verification. The registration process provides the facility to choose the factors for verification belongs to a user called by authentication credentials like password, pass-phrase, one-time password (OTP), etc. The verification process verifies the user’s identity through the authentication credentials at the other end, that is, generally a server. Therefore, authentication credentials are factors/properties/attributes that make it possible to verify the identity of the user [9,10].

Multiserver identification techniques

Current life is dependent on various services based on ICT. The quick development and deployment of innovation using Internet are pushing the current technology in direction to the IoT, that is, Internet of things [11]. For the IoT-based systems, one of the big challenge is security. Therefore, the emerging technical fields are required security in terms of integrity, confidentiality, authentication, availability, etc. Among of these security services, authentication is an important security service. It is a process to verify the truthfulness of the user who requested to access the specific sever or its services. Very initial authentication techniques are based on

one-way hash function which is proposed by Lamport *et al.* [12]. But, it failed against interpolation attack because of verification table maintenance [13]. To provide resistant and protection against the identified interpolation attack, Chang *et al.* developed a new scheme for authentication. This scheme was provided a password authentication for remote user and used smart-card and resistive against the interpolation attack because this technique did not use any verification table [14,15]. There are various other related schemes are also available in literature, but a section of these schemes are dependent on static and fixed user's identity [16–18]. These techniques are not resistive for the information (related to user's authentication) because this information is static in nature. M.L. Das *et al.* proposed a new concept for authentication which is based on dynamic ID of the user rather than the static ID as in previous listed techniques in 2002 [19]. Later other similar techniques are also proposed which are based on dynamic-ID of the remote user [13,20–22]. There are various security attacks identified for these dynamic ID-based authentication schemes as identity theft attack, etc. Then, a new authentication scheme is proposed by the Leu *et al.* in which a user identification and a key distribution scheme was proposed which was based on the method of factor and a hash for multiserver environment [23]. As technology changed the services are not only depended on single server. Multiserver-based authentication schemes are come in picture, therefore, new authentication techniques are evolved which are based on multiserver environment. In 2009, Liao and Wang created a new authentication protocol for multiserver environment based on dynamic ID of the remote user. The ID of the user is dynamic and changes dynamically which is called as dynamic ID for this scheme [17]. This dynamic ID-based technique was resistive for various attacks and provided various security services as mutual authentication and sharing of the session key. Lee *et al.* [20], Li *et al.* [24], and Xue *et al.* [25] have proposed related techniques of user authentication for a multiserver environment. One better, more practical, secure and efficiency techniques was proposed by Leu *et al.* which used hash function in its implementation [23]. There are various important symbols used to explain the technique of authentication explained as Identity of User is ID , Password of User is PW , Hash function $h(.)$, Bitwise XOR operation is $\oplus$, Concatenation operation is $\parallel$, Secret value of the server (to be stored on the smart card) is y , Secret value of the server is x and Service Providing Servers identity is SID_i .

In this section, following techniques are identified. These techniques are:

1. Lee *et al.* scheme
2. Li *et al.* scheme
3. Xue *et al.* scheme
4. Leu *et al.* scheme

Lee *et al.* scheme: This protocol is used for a multiserver environment with three entities as the user (U_s), the SPS (S_j), and registration server (RS). In this technique, user chooses b as a random number along with a password PWD_i . The detail communication between these entities are given in Figure 4.3. All the parameters are shared among these entities through secure channel and x (the master

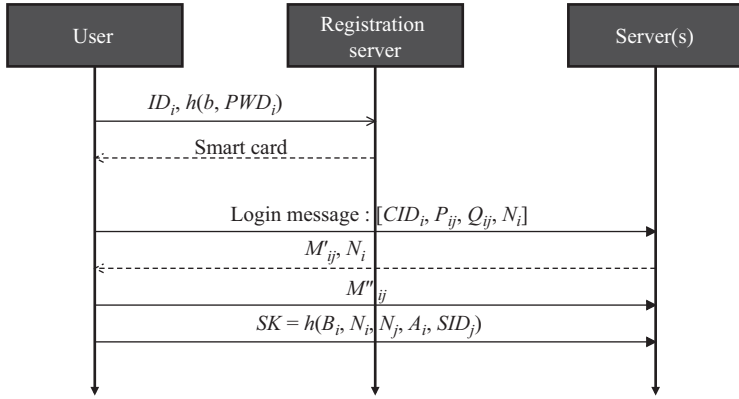


Figure 4.3 Sequence flow of Cheng Chi Lee [20] authentication protocol

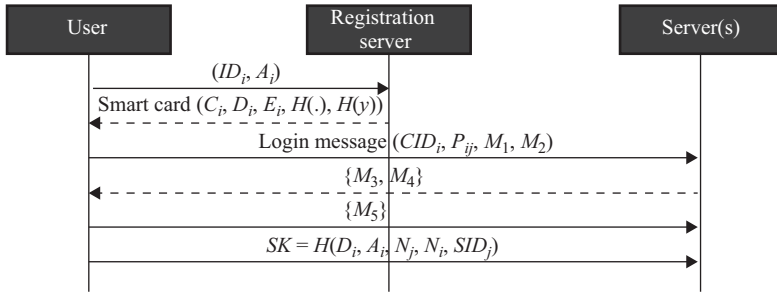


Figure 4.4 Sequence flow of Xiong Li, Jian Ma et al. [20] authentication protocol

secret key) and y (secret number) are only known by RS. The detailed analysis is given by Gahrana and Anand [26]. CID_i is the parameter saved on smart card along with other parameters as mentioned in above discussion. To resist time-related attacks nonces are generated at server and user as N_j and N_i , respectively [20]. At the end, SK (session key) will be generated at both the ends as shown in (4.1):

$$SK = h(B_i, N_i, N_j, A_i, SID_j) \quad (4.1)$$

Li et al. scheme: Three layers user (U_i), the server to provide services (SPS) (S_j), and registration server (RS) are established an environment for this protocol [13]. The detailed working of this protocol is given in Figure 4.4. The detailed analysis is given by Gahrana and Anand [26]:

$$SK = h(D_i, A_i, N_j, N_i, SID_j) \quad (4.2)$$

Finally, SK (session key) will be generated at both the ends as shown in (4.2)

Xue et al. scheme: Similarly as the above-mentioned techniques, Xue et al. also engaged three layers as a user (U_i), the SPS (S_j), and CS, that is, control server [27].

Figure 4.5 shows the detailed sequence diagram of this protocol and calculations are as

TS_i is current time-stamp value at U_i . The detail analysis is given by Gahrana and Anand [26]:

$$SK = h((N_{i1} \oplus N_{i2} \oplus N_{i3}) || TS_i) \quad (4.3)$$

Finally, the session key, that is, SK will be generated as shown in (4.3).

Leu et al. scheme: A random number is used by this protocol which is involved in it make difficult to illegitimate access to the system. Figure 4.6 shows the sequence diagram of the protocol as the detailed analysis is given by Gahrana and Anand [26]:

$$SK = h(O_i || A_i || SID_j || N_i) \quad (4.4)$$

Finally, the session key, that is, SK will be generated at both the ends as shown in (4.4).

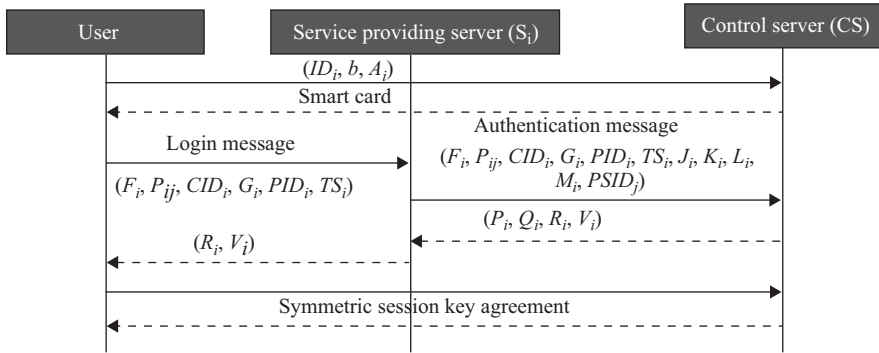


Figure 4.5 Sequence flow of Kaiping Xue et al. authentication protocol

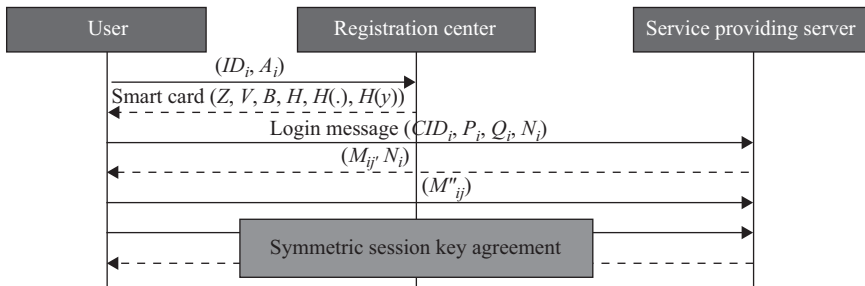


Figure 4.6 Sequence flow of Leu and Hsieh authentication protocol

Analysis of multiserver identification techniques: The analysis of the above explained techniques have been done on the basis of some attacks. Further the techniques can also be analyzed on the basis of computation overhead and communication overhead too. For the sake of understanding, the analysis is only provided in term of proving the resistance of the techniques for security attacks.

The analysis of the above-discussed schemes is presented in the Table 4.2.

Table 4.2 Details of the security analysis of mentioned schemes

Attack	Description	C.C. Lee	Xiong Li	K. Xue	Li and Hsieh
ID protection & user anonymity	User ID (Pseudonym identity [25] and Dynamic ID [28]) protection against malicious attackers	✓	✓	✓	✓
Traceability	Real identity of a user is extracted and able to extract further linked dynamic and pseudonym identities [29]	×	×	✓	×
Mutual authentication	Breaking of the functionality an identity proved by client and server to each other	×	×	✓	✓
Session key agreement	Session key ensure the security of the communication of a correspondence session among a client and server	✓	✓	✓	✓
Password updating/ changing	Update and change users password whenever required	✓	✓	✓	✓
Insider attack resistance	Administrators and other approved people may abuse the system	×	×	✓	×
Resistance of stolen smart-card attack	Attacker can extract secret information, break the system, and derive sensitive and secrete information from the stolen smart-card.	✓	×	Prob	×
Resistance of replay attack	Intercepting the previous messages and after that replaying them to the expected end of the communication system	×	×	×	×
Denial of service attack	Intercepts the normal operation of a server using flooding with several packets	×	×	×	×
Resistance of eavesdropping attack	The interception of exchanged messages between the entities from communication channels	×	×	×	×
Resistance of masquerade attack	Intercepting the communicated messages among various communicating parties and then storing them for replay	✓	✓	✓	✓

4.3.3 Authorization

Definition 3: *Authorization is a positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified.*

In other word, authorization is also defined as:

Definition 4: *“The granting to a program, a process, or a user the right of access”*

Authentication is simply the gate-pass to enter in the secure system. The system has a number of services and for each service, various rights are available as read, update, delete, etc. Therefore, after successful authentication, the process of authorization is executed. The objective of the authorization is to evaluate the authenticated request and permits the user to access the services of the system according to its role. Every organization publishes their policies for authorization and the authorization controls the access of user according to these policies. Generally, an access control list (ACL) is to be used for authorization which specifies the mapping of the rights of operations to the users. Each event triggered from the user’s end is for accessing a specific server required proper rights and for this authorization process lookup into the ACL. According to the entry in ACL, the system is allowed the user to access the requested services [30].

4.3.4 Access management

Definition 5: *The mechanism to manage the access control of the various resources including systems, services, and applications within an organization including user account management is access management.*

The identity of a user is related to the access management of various resources. For example, a *student* (user identity) has a *course* function that requires access to certain resources. The permission to access is granted using a combination of linked accounts (e.g., user account) and access controls of various system resources. The objective of the integrated identity and access management (IAM) is to develop a mechanism which is the combination of software technologies and business process, to control, manage, and provide secure access to sensitive resources and information within an organization. It is a very good practice for business organizations. Along with this, some organizations are regulated through security compliance requirements which are the main target of IAM. These security compliance requirements are playing the vital role for the users looking to deploy an integrated IAM at their servers. For example, suppose, if a client/customer wants to ensure that all the identities of the users are removed which do not have any current link and relationship with the business. This can be met through security compliance and works as a security compliance requirement through which the IAM restricts the users who no longer have any connection with the client’s business [31,32].

Objective of access management: The objective of the access management is to provide the rights to use a group of services for a user. Therefore, the access management is the implementation and execution of the user-access policies such that the action of these policies can be defined in information security standards. The objectives of the access management is explained as follows:

- The process which allows authorized user to access the service and simultaneously restricts the nonauthorized users to access the same services is called Access Management.
 - Allows a user to access the service group, services, functions or data.
 - The users get rights to access the services only if they are authorized to get access to these services.
- Another objective of the access management is to identity management or rights of management in light of Protecting Confidentiality, Integrity, and Availability (CIA).
 - Remove or update the access right of a user when the roles or jobs of the user will be changed.
 - Remove user who no longer related with the organization.
- Various incidents and problems related to security and access management will be discreetly recorded.

The scope of access management: The effective execution of the availability and information security management is the scope of access management. The access management enables the organization to ensure and manage the confidentiality, availability, and integrity of its intellectual property and information. The process of the access management can be initiated by a request to access the service through the service desk.

Elements of access management: Following entities are interacting with the IAM system:

Security architect: The security architect is responsible for establishment of the security policies and its implementation for the organization and it further maintains, manages, and control it. The security architects are also responsible to meet the requirements of the business through IAM. Some of the important facts about it are as follows:

- Implement the technological solution to achieve the business goals such as:
 - Business to Employee (B2E): To enhance the applications for employees using ICT.
 - Business to Business (B2B): To provide platform for integration with other clients and other business partners.
 - Business to Consumers (B2C): To exercise the opportunities with consumers through the internet to extend the business.
- Align the security requirements to the business policies of the organization and further define the evaluation metrics will be exercised for these requirements using the technologies related to the information security.

- Integrate and deploy the security-related technologies over the existing environment of the client.
- Monitor and manage the deployed security environment through a proper deployment strategy to make it consistent, consolidated, and centralized.

Internal employee: The internal employees are an important users who deals with day to day application, transactions, and events of an organization. The Single Sign-On (SSO) facility is provided to the employees through IAM. This SSO facility enables the internal employees of the organization to feel consistent and ease of application on the computer enabled system. The IAM also enables internal employees to execute self-service within the limits of the approved policies for compliance in the organization. The goals of the internal employees are proposed through IAM are as follows:

- Provide permission to internal employees to access various accounts and applications which are required to perform their jobs.
- Enable internal employees to perform following the important process and activities within the security framework as:
 - Self-service through SSO
 - Activities related to the password as:
 - password expiry
 - password change
 - renewal of password
 - forgotten password

External customer and partner: External customers are the people/organization that pay for and use the services or products of the organization whereas partners are the people/organization which have the alliance to do various activities of the organization. Therefore, similar to the internal employees, the external customers and partners are also be benefited from the IAM. The goals of the IAM for external customers and partners (ECP) are as follows:

- Facilitate the above-mentioned stakeholders to access the external application and facilities of the organization.
- Enable external customer and partner to perform the following important process and activities within the security framework as:
 - Self-service through SSO
 - Activities related to the password as:-
 - password expiry
 - password change
 - renewal of password
 - forgotten password

IT administrator: These are technical people who work with security architects. The goals of IT administrator for IAM are as follows:

- Ensure and control the access of the users such that the applications are accessible only to the authorized users.

- Ensure the policies about the account management for accounts on a system such that, it will be accessible only to the authorized user.
- Ensure that the other stakeholders like external customers, partners, internal employees, etc. will be able to use password-related activities, self-service, etc.
- IT administrator also handles the following changes as:
 - Joining of new employee
 - Changes of the last name and other information for the employees
 - Change of department of employee
 - New application protection

Application owner: The primary responsibility of the application owner is to provide approval to the user's request to access the applications which they owned. The goals of application owners from an IAM system are as follows:

- Register all the complaint related to security audit reviews.
- The valid request will be approved to access the applications which the *application owner* owned.

Employee manager: The responsibility of the employee-manager is to approve the requests which are related and linked with the events of identity life-cycle management of the employees. The goals of the employee manager's are as follows:

- Register and track the status of the complaints related to his/her department with all reviews of the security audit.
- Provide approval to access systems and applications from their related employees by the authorized requests.

4.3.4.1 Access management activities

Requesting access: The mechanisms to request access to resources are as follows:

- Request in a standard format.
- The change request.
- The authorized request to access a service, that is, service request.
- Mechanism to make a request for authorization, that is, preauthorize request.
- Manage the rules from the service catalog for providing access to the request.

Verification: Verification is a subprocess of access management to verify each request which is requested to access the IT services. There are two major perspectives as:

- Verify the identity of the user to access the IT services.
- Verify the requirement in such a way that it has the legitimacy to access the services.

Providing rights: Access management is not responsible to make a decision about the legitimacy of the user. It is not able to decide who will access which service. It implements and executes the regulations and policies decided during the design of services and its strategies. While access management is responsible to

restrict the access to the unauthorized user rather than decision making about the legitimacy of any user. After verification of the user's legitimacy, access management will provide the rights to the legitimate user about the requested services. For this, various departments and teams are involved and they will work automatically to support this service to make necessary action.

Monitoring identity status: The change of roles and working of the users impacts the access of the services. These changing of roles and working are due to death, change of job, demotions, promotions, etc. These changes will be reflected in life-cycle of the user. Therefore, access management is implemented in such a way that it is able to understand the user life-cycle and its changes. Further, the access management is able to implement these changes automatically in the system. It is also important to provide a feature in access management process which enables the user to migrate from one place to another place and also write log to the audit trail for the purpose of the security audit.

Logging and tracking access: Apart from responding to request, the access management ensuring that the rights are being properly exercised by the user. The information security management (ISM) is responsible to detect, authorize, and unauthorize access. ISM also compares the unauthorize access request with the rights provided by the process of access management. The vulnerabilities of the various services are easily identified through this exercise. Therefore, access management needs to provide a record of the access to specific service during any forensic investigation. This record is useful for the following reasons:

- To identify the user who is suspected due to breaches of the organization's policy.
- To identify the inappropriate use of various resources.
- To identify the data which is used for fraud.
- Provide date and time for evidence.
- Provide contents about the user's access of service by an unauthorize user.

Access management components: To design and implement an effective IAS, three key components are to be understood and analyzed as follows:

1. Users
2. Assets
3. Privileges

Users: Users are the entities to use, manage, control, and manipulate the assets/resources/information using the rights to access through user-access management. To protect these assets/resources/information from the unauthorized user, user-access management implements the mechanism of access control. It is the mechanism used to ensure the accessibility of the assets/resources/information to legitimate users. The users can be categorized on the basis of its role and duties according to the policy of organization as for hospital the user may be doctors, patients, administrative staff, nursing staff, etc. The services are also categorized for these set of users. So, the objective of the user-access management to map the various services for its user's set.

Assets: All assets in user-management are always fallen under the scope of consideration for any organization. These assets are being protected through a deep defense strategy. The assets at the high level are as follows:

- **Physical:** These are hardware devices, mobile devices, including workstations, servers, printers, USB devices, switches, hubs, routers, wireless access points, and other related physical systems including electric devices used to run access management system.
- **Intangible:** These are operating systems, file systems, strategies, standards, audits, network-based applications, host-based applications, web-based applications, etc.
- **Information:** These are linked with stored information like data storage.

Privileges: Privileges are the set of authorizations which dictate the actions that can be performed on organization assets by a legitimate user. These privileges can be controlled or restricted through the criteria of access as follows:

- **Identity:** The access control based on the user's identity.
- **Roles:** The access control based on the user's role.
- **Location:** The access control based on the physical location of the user; like, some services are accessible only within the local network.
- **Time:** The access of the system based on the time; for example, some services are accessible only during the office hours.
- **Transaction:** The access control based on the action; like, the issues related to open ticket is visible to the user but when the status of the ticket is changed to close, it is not accessible.
- **Access modes:** Access control based on user's access mode; for example, write, delete, or read-only mode of access.

Roles: The "role" in access management is used to refer to the membership of a set. This set belongs to the specific access requirements for all the members. A user of the system may have many roles and on other side, many users may have a single role. Never be confused about the term "*Role*" with "*titles*" or "*positions*" for an organization. The role engineering method is responsible to derive the roles and it can be described as follows:

- Various possible scenarios are identified for system usage and then modeled them for implementation.
- Identify the requirements about permissions for above-mentioned scenarios with minimum possible actions for each scenario.
- Identify the constraints for each permission which are necessary to implement the role like dependency on time, separation of responsibilities of the user, etc.
- Developed scenario-model will be reviewed and generalized in possible subscenarios.
- Define profiles and tasks where tasks are the group of profiles and scenarios are the groups of tasks.
- Develop a role hierarchy with the use of work profiles and permissions which are already defined.
- Define role-based access control (RBAC). In this model, the removal of the redundant roles is possible. Based on the analysis, new hierarchies of roles and constraints can be developed, separated, and merged [33].

Threats to access management: The ultimate object and outcome of the IAM are to establish a “*gateway*” through which all the requests will be processed. This “*gateway*” has a responsibility to stop the unauthorized requests and the authorized requests can be passed to access the resources. To test this “*gateway*”, an environment needs to be created which includes a significant range of targeted attacks is called threat environment or threat model. This security testing using the threat model is very important to certify the IAM on the basis of various standards attack [34].

4.4 Policies for identity and access management

The policy of identity and access management (IAM) defines the permission for action which is used to perform actions for access management. For example, a policy permits the action of the method “*getUserInfo*,” then the user with this policy can access the user information through this method from the IAM console. The vulnerabilities in policies of the IAM is generally depends on the following elements:

- *People*: The human factor
- *Technology*: Access control services and its technical aspects
- *Process*: Management of the processes in poor condition

The human factor: There are four pillars of defense as governance, people, process, and technology and people is the weakest link among of these. Generally, the assessment and control are most difficult for acknowledgment of people. Because of these difficulties, the people will become a proxy for malicious attack. In 2007, according to a study of Deloitte, 79% participants of the survey cited that the human factors as the root cause of failure of the information system. This is because of the small errors which lead the system to disclosure of the sensitive information. Further, this error leads the system to inadvertently opening vulnerabilities which provide accessibility of sensitive information to the attacker. Such errors are responsible for:

- Disclosure of sensitive information at a public platform like the Internet.
- Send the sensitive information (like financial data or credentials) to unauthorized entities.
- During the processing of documents, the system failed to carry out sensitive information, management procedures, or operational data.

Technical aspects of access control: Generally, the security to the access control can be provided by enforcing the technology, strictly over the defense layer and analysis should be taken in depth. There exists many cases where the access control is vulnerable for security attacks and the access control system is compromised due to it. There may exist weaknesses due to the following reasons:

- Weakness in development and design
- Weaker configuration
- improper security testing of controls
- issues with suppressed systems

There are a number of technologies related to management of user-access which are suffered from incorporate trade-offs or suffered weaknesses of usability against information security paradigm. Some the examples are as follows:

Single sign-on: It is a process of authentication for the user using single set of authentication credentials for authorized services. The drawback of this process is that, there is single success as well as single failure point. Therefore, due to severity, more attention to manage and secure this point of entry. The target should be to protect the system from various attacks and provide the simple and easy facility of the authentication using single sign-on process.

Biometrics: The use of behavioral or physical properties of a personnel as credentials of authentication also are vulnerable to security risks. The initial testing has inferred that biometry is also susceptible to repeating or fraud, and once impacted through unauthorized access will never be undo, significantly if denote on a public forum as proven by the knowledge of a German executive director, whose fingerprints square measure currently downloadable freely. moreover, on condition that repeating biometry needs physical proximity.

Multifactor authentication: To provide more security, the multiple (generally more than one) factors are used for authentication of any user. This type of authentication is providing the more security in comparison to the traditional and one factor authentication techniques. But, if these techniques are implemented incorrectly then it may cause various weaknesses, particularly in matching of credentials. All the factors should be interdependent, if these factors are taken separately then it may cause of unauthorized access as the factors are checked only for validity not checked for interdependency of various factors.

Remote access solutions: Intercommunication technologies provides productivity and flexibility to the employees of any organization but the remote accessibility of any system accessibility including increases the probability of attack to the system. If authentication and accessibility of the user are not adequately managed then attacks may occur.

Poor management of processes: Targeted, clearly and specific policies and mechanism should be consistent, well documented, and sustainable for operations for user-access management. The vulnerabilities are existing in the system because of the poor and weak design and policies and operations which are required for user-access management-related tasks. The well-defined, properly analyzed and tested designs, policies, procedures, and operations should be followed by the users to avoid the security hazards but apart from it, these are probable reasons as follows:

- Malicious intent
- The considered processes may be resource-intensive
- Possible real error

If the users do not follow the desired rules, operations, and procedures due to any reason then the related assets will become susceptible to compromise. The reasons for arising vulnerabilities in general are include:

Creation of user account without any approval: The creation of the user account during this manner is also available for malicious activity. Albeit generated

for secure use, the accounts could have incorrect access privileges that can be abused by alternative parties.

The deletion of test accounts after usage: Test the user accounts sporadically which possess upper levels of access to the systems and connected data and area unit usually in some way allotted to people. Processes that don't apply for the killing of privileged accounts are in danger.

Access privileges not changing commensurately with internal role changes: When users amendment positions inside associate degree organization, there nearly always are a amendment within the access privileges needed, whether or not increasing, decreasing, or a whole remapping of associated roles and privileges.

4.5 Security attacks and goals

The evaluation of any security algorithm, process, or mechanism is important. For this evaluation, the security mechanism is tested for security attacks and security goals. The security attacks are countered by the reactive events. On the other end, the proactive events are embedded within the algorithm during the design and development for security goals [35]. So, the generally accepted security goals and security requirements are given in Tables 4.3 and 4.4.

Table 4.3 Security requirements (SR)

S. No.	Security requirement	Detail
SR1	Eavesdropping attack	Attacker cannot extract the private security information from eavesdropped messages over public channels
SR2	Masquerade attack	The malicious attacker cannot forge other users identity like smart-card/PIN/etc. from known security information
SR3	Denial of service (DoS) attack	The system may crashed by a number of unwanted requests generated by malicious attacker. On the basis of this difference validation of the request will be done
SR4	Forgery attack (impersonation attack)	The malicious attacker can access the stored information on a smart-card and further forge a new smart card [36]
SR5	Parallel session attack	An attacker can masquerade the session as a legal user without any knowledge about authentication parameters like user's PIN, etc. [37]
SR6	Password guessing attack	Due to guessing of the password, an attacker can access the system as a legitimate user [38]
SR7	Replay attack	Attacker captures the message and retransmit the message without any change [39]
SR8	Smart-card loss attack	If malicious functioning will be taken place due to loss of smart-card [40]
SR9	Stolen-verifier attack	Anyone can steal the password verifier like hashed password then, the user masquerades as a legitimate user [41]
SR10	Reflection attack	Same process and mechanism is used in both the directions to authenticate each side [42]
SR11	Insider attack	Malicious user knows some legitimate information try to access the user's information and compromise the system

Table 4.4 *Security goals (SG)*

S. No.	Sec. goals	Detail
SG1	No verification table	System should free from a specific verification table which stores the password and authentication credentials as a plain text [43]
SG2	Freely chosen password by the users	Providing the freedom to the user about the selection of the password
SG3	No password reveal	Sensitive credentials for the user authentication (like password, etc.) should not reveal during the registration process
SG4	Password dependent	The authentication process should directly and only depends on password only
SG5	Mutual authentication	Both parties can share the session key not only for secure communication but also for authenticate to each other
SG6	Session key agreement	The session key agreement is to provide secrecy of messages between the communicating parties
SG7	Forward secrecy	To stop the impersonate the user to login to the system by the attacker [44]
SG8	Smart-card revocation	If smart-card missed or lost then there should be a provision in the system for invalidating the further use of the lost smart-card, otherwise an adversary can impersonate a validity registered user [45]
SG9	Efficiency for wrong password login	If the user inputs the incorrect password by mistake in login phase, without any delay the IAM notifies the user with an error message

4.6 Identification and access management techniques

Identification and access management techniques (IdAM) depends on the architecture to manage various processes and functionalities of the IdAM. The basic architecture of the IdAM is illustrated in Figure 4.7.

There are seven processes to support, manage, and monitor the functionalities of IdAM as follows:

USER registration: This is the very first process to execute for IAM which determines that there should exist a reason to a user. This reason is providing the ability to access the resources after verification of the person's identity. This process is useful to create one or more identities for a user.

Credential issuance and management: This process provides the life-cycle management of credentials, such as employee badges or digital certificates. Additional information on credential issuance and management, as well as authentication, can be found in NIST SP 800-63-2, Electronic Authentication Guideline.

Access right management: This process provides the access right management to the system which determines the resources that a digital identity is requested and allow to use.

Provisioning: This process populates credential, digital identity, and access rights information for use in access control, authentication, and audit.

Authentication: Authentication is the proof of the user's claimed identity and also establishes confidence in a user's digital identity.

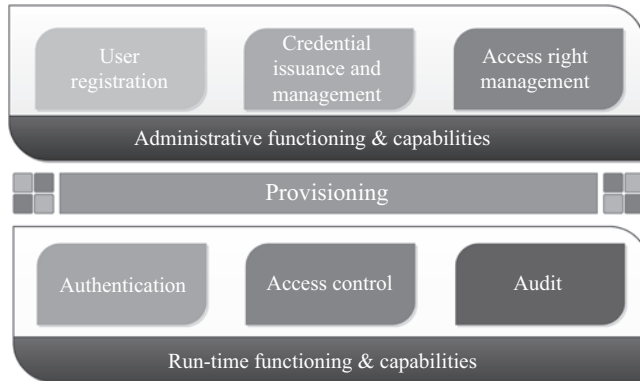


Figure 4.7 General architecture of identification and access management

Access control: Access control is a process which allows or denies a digital identity access to the services and resource.

Audit: Audit is the process to maintain a record of the resource access attempts by an authentic user.

4.6.1 Identity management techniques

IAM is processing in which people, processes, and products will be managed user's identity and access to resources within the organization, and can be classified into three common models.

4.6.1.1 Isolated identity management

Every service is isolated and will be accessible only when an authorized user request for it and which possess a user's identifier to access these services. This type of model is useful generally for the systems which are implemented in such a way that the services and other resources are available online for the users. It is easy to implement the systems based on this model because it is relatively simple for the service provider and resource management but on the other end it is quite complex and unmanageable for the user to manage and get access control for various other services which are not available in the access right of the current user. Users are being overloaded with authentication credentials and identifies for a number of services. This is because of the exponential growth and popularity of the online services. Therefore, the user needs to remember a number of login credentials (like username and passwords).

4.6.1.2 Federated identity management

Federated identity management (FIM) simplifies the problem of management of the user-account. For the identity management in this model, a set of standards and agreements are identified and defined in service groups. The main responsibility of these groups is to recognize the identity of the user from one another. A user of one kind of service could access all other services provided by the other services of the same group with a single authentication identifier.

4.6.1.3 Centralized identity management

This model uses the central authentication repository or service which is used by each service provider for the purpose of identity management like a public key infrastructure (PKI) where a certificate authority (CA) issues the user's certificates for identification which will further use for access management. This certificate will be used by the user for access other services. The CA will be responsible to validate the authenticity of the user. The other example is the single sign-on (SSO) model in which user login to a system once and be authenticated for other services automatically. Other examples are Kerberos Authentication Server, Microsoft. Net Passport, etc.

4.6.2 Access management techniques

To determine the access permissions to get access for specific services and resources, a mechanism is used which is called by access management. Following are the common access control models as follows.

4.6.2.1 Discretionary access control (DAC)

In this mechanism, all the resources and objects are under the control of user. The revoking and granting access to the system are depending on the discretion of individual users.

4.6.2.2 Mandatory access control (MAC)

Based on the sensitivity of the data contained in the objects, this mechanism used to restrict the access of these objects. The accessibility of the sensitive information is provided only based on the formal authorization.

4.6.2.3 Role-based access control (RBAC)

In this technique of authorization, the roles are given to the users to access the services. Based on these roles, the user can only access the specific services.

4.7 Identity and access management of e-healthcare systems: case study

E-health care or electronic health care is an application of information and communication technology (ICT) for delivering cost-effective health services by any country or organization to its citizens or clients with reliability, transparency, and efficiency. It is integrated service of various other health and other services through various servers. As far as identification and access management is concern, the research directions of e-healthcare systems can be divided into two categories as:

1. IoT-based healthcare security
2. Smart e-health gateway

4.7.1 IoT-based healthcare security

In literature various healthcare system are explained [46]. The Harvard sensor network lab has been developed the healthcare research project "*CodeBlue*" which becomes one of the most popular among all the related systems. In this project, a

number of sensors are placed in the body of the patient. CodeBlue is developed and deployed with the expectations that it will work in emergency situations for the patient where disaster response and rehabilitation are required. CodeBlue developers have admitted the necessity and requirement of security for medical application-based on IoT and the security aspects are still pending for future. While Lorincz *et al.* suggested that elliptic curve cryptography (ECC) and TinySec are best suited for this project to be used for session key generation and encryption (symmetric) for secure communication, respectively. These suggested solutions are still pending and not implemented yet. For evaluation and testing of security, Kambourakis *et al.* discussed attacks models and threat model for this project [47]. Some of the key points related to this security analysis as follows:

- Denial-of-service (DoS) attack
- Attack of snooping
- Grey-hole attack
- Sybil attack
- Masquerading attacks

The data are transmitted regularly in this project between peers, therefore, to establish network security between end-peers of the general end-to-end security protocols are recently proposed by DTLS. Datagram Transport Layer Security (DTLS) is one of the protocols and most related one to the above mentioned problem. Hummen *et al.* proposed and presented an implementation of the delegation architecture system which is based on an off-path delegation server as shown in Figure 4.8. This architecture which is based on delegation architecture relies on a centralized delegation server but this architecture failed to provide scalability and reliability. This environment will not be extended to be implemented for the systems of multidomain. This system is affected generally due to considerable network transmission which enhances the overhead. Ultimately, this situation impacts the system as a long transmission delay. Moreover, if a malicious user or attacker performs a DoS attack or compromises the delegation server, this DoS attack can hamper the security of not only this project but also disrupt all the constrained which are available for medical domains as shown in Figure 4.9.

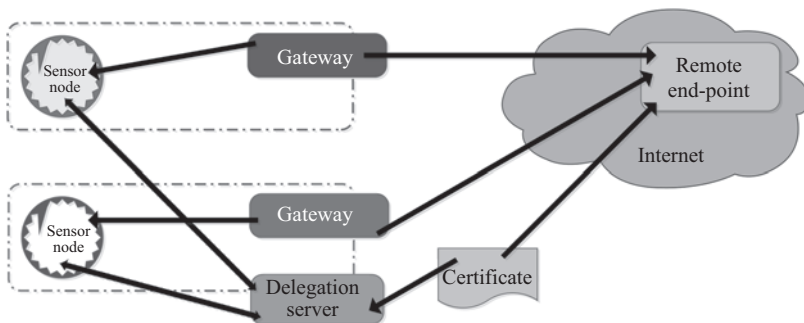


Figure 4.8 IoT-based e-healthcare monitoring system architecture using e-health gateways in hospital/home domain(s)

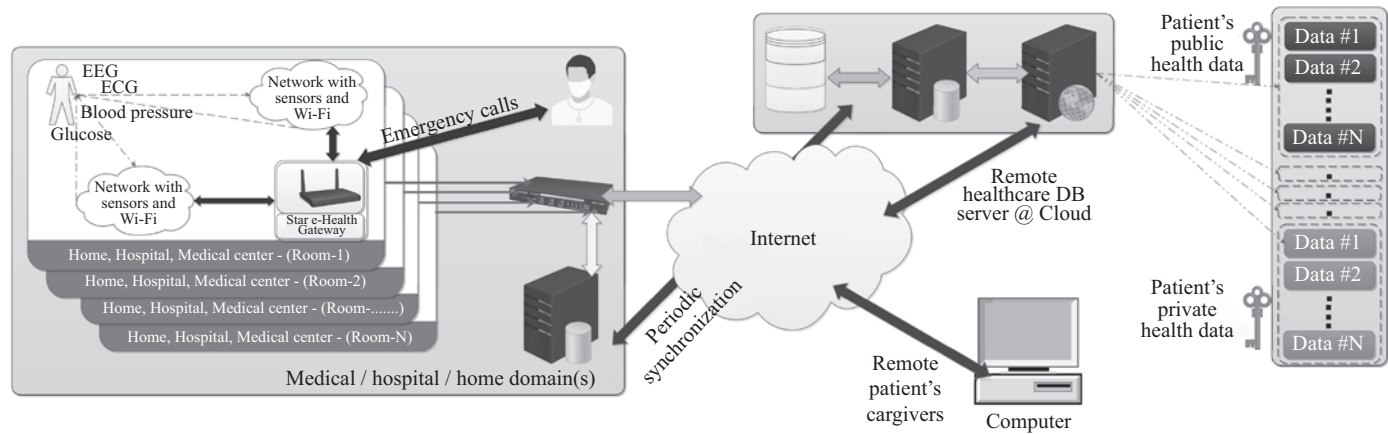


Figure 4.9 The architecture of an IoT-based healthcare monitoring system using smart e-health gateways in home/hospital domain(s)

4.7.2 Smart e-health gateway

To design the gateways, a number of efforts are required for single or many applications and architectural layers. The *SwissGate* gateway is presented by Muller *et al.* which is used to handle the operations of sensor networks and also optimize the operations. This gateway successfully deploys for the home automation applications transparently. This gateway is supposed to deploy for the e-health care system. There is a big problem because of the reason as for how the data will be routed in the IoT system where data exchange will be taken place using a huge number of sensors. Shen *et al.* proposed a prototype for this type of communication, that is, *smart 6LoWPAN*. Rahmani *et al.* present *UT-GATE* which is e-health gateway includes a smart functioning to apply intelligence for the ubiquitous healthcare systems based on IoT. These gateways are offering basic services at the edge of the network. Therefore, these gateways helped to remote cloud computers to provide services which are often required to access to the central database and computationally intensive in nature. Figure 4.8 illustrates a smart home/hospital where the gateway is in a specific position between the Local/Patient/Body Area Network (LAN/PAN/BAN) with Wide Area Network (WAN) [48]. Due to a huge number of connections and communications in the system, it will be exploited by various means. Therefore security is required for the gateway from where communication takes place. So, the smart e-health gateways supported by sensor network using the Internet are empowered with the facility that processing of various resources, memory, communication bandwidth, power consumption, etc. without any constraints but it will be secured for malicious attacks. For this, DTLS handshake based on the certificate is deploy for the security purpose specifically this security is related to authentication and authorization.

4.7.3 Implementation components for the e-health care system

This section is trying to focus on the components which are required by any e-healthcare system. These are as follows:

Human resource considerations

- Clearly define and document the security about agents, patients, service providers, employees, etc.
- Check criminal records for all.
- The process to verify the academic records, prior experience, professional skills, and qualification.

General access controls

- All the persons willing to participate in any process will be verified through its identities.
- As per discussed policies and documents for requestors business needs, it is a must to ensure that all the access to the systems should be provisioned.

- There should be restriction or limitation to the objects, resources, information, files, etc. of the system.
- The user ID should be traceable for all the users and, using this ID; Service ID will be traceable for the information system.
- There should be the ability of the system to configure its IDM and access control services.

Administering IDs

- The creation and changes of the various e-healthcare systems should be managed.
- To handle various requests, there should be an electronic or written process. This process will not be work without the associated ID which will be created through an automated process.
- The details of sponsors should be entered in the system. This details may contain full name, sponsor authority, department, location, and other important contact information.
- Each and every request should be justified by the proper reason and enterer in the system. Further, each request should be associated with a unique ID if applicable.
- All the IDs are listed and managed by a program or process.
- Privileges associated with the ID.
- The termination, contracts, or other relationship should be governed by a policy. This policy will be shared to concern persons through a system.

Privileged IDs

- Privilege level and other personal information associated with any ID must be hidden for security point of view.
- The assignment of any privileged entitlements must not be done on the personal ID in the information system. Official ID should be used.
- For any privileged access to the system, all the persons should use their privilege ID.
- Privileged ID is used only for the limited number of users who are directly linked with operation or administration. The system should ensure its limited assignment.

Service ID

- The program is developed in such a way that the service IDs are unique and different from the service ID created by the information system.
- It should ensure that these Service IDs are not vulnerable for any interactive attack for authentication.
- The providing Service IDs may use nonexpiring password so that these IDs are incapable of being used by any attacker.
- It should have capability to change and update the password of credential associated with the Service IDs.

Authentication

- For the purpose of authentication, the credentials (password, passphrase, etc.) should be communicated to concern person securely. If an ID has been sent through email then associated credentials must be communicated by an alternatives like phone, SMS, mail or other email ID, etc.
- The initial password should be changed and this process will be mandatory for all the IDs. On first login, user must be delegated to set password or change password platform so that the user will set their password.
- The authentication credentials must be masked. For example, to login, user provides its username and password then password is masked using “*” character. To check whether the entered password is right or wrong, temporary visibility facility may be given for a while.
- There should be a password policy in which the combination of characters, length of the password, life of the password, etc. has to be decided. Further, there should be a process/program to ensure and force this password policy.
- To reset the password, there should be a process in which user’s ID must be verified prior to the process of changing of it.
- Program must encrypt passwords in transmission.
- Program must not cache decrypted passwords.
- Program designed in such a way the password will not be saved as plain-code, hard-code, simple-text, etc.
- There should be program to ensure the backup or contingency through paper-based passwords. This should be done using the technique of split knowledge or dual control.

Sign-on controls

- The program is developed in such a way that, the banner or message must be displayed prior to the authentication of the user. It should be ensured that, to access the system and executing the process of authentication, the terms should be accepted by the user.
- The reason of failure of the e-healthcare system will not be indicated like not existing of ID, incorrect password, etc.

Default IDs and passwords

- All the IDs should be registered at the system and for this, there should be a program to ensure the registration of all the default IDs of vendors and provide renamed these.
- Default or null passwords must be changed or set by a program before implementation of the system at the production server. It should be tested at test environment prior to the deployment at production.

Remote access

- To access the system remotely, it should be ensured that additional authentication factors should be applied through untrusted sources.

- Remote access of the system will be permitted only at the virtual workspace computing solution approved by the e-healthcare system.
- There should be a program to maintain all the agent records and various services.
- This service provides the remote access to the server only for the authorized users.
- Program to ensure integrity and confidentiality of all the sessions of all remote access connections should be employed cryptographic solutions.

Session management

- For session management, the system is programmed in such a way that multiple concurrent sessions will not be established through personal IDs.
- The system is programmed in such a way that multiple concurrent sessions will not be established through privileged IDs in the system.
- The system is ensured that established session must be controlled by the system.
- The session confidentiality and integrity of the session will be protected by the program implemented in the system.
- The established session will be associated with unique session ID and the validity of the each session will be ensured for a finite duration. This functionality will be ensured through a program integrated with the system.
- The facility to end or termination of the current active session will be programmed and integrated in the system.

Enforcement

- The oversight body (which is applicable) will be authorized to review all the noncompliance instances.
- The applicable oversight body is authorized to impose appropriate penalties, etc. This body is also authorized to terminate the agreement with electronic service providers and HIC, and requires the remedial actions for implementation.

4.8 Summary

The IAM is very important technique for any information system. It will become more important when the information system is deployed using the ICT over Internet. Authentication is one of the very important security service according to ISO security standards. E-healthcare implementation is a big challenge for any country due to larger manpower. The challenge is becoming more complex when the diversity of the region is exercised. Further the e-healthcare solutions are providing a number of services. Therefore authorization is also very important to give access to legitimate users. This chapter explained the basic and technical concepts of IAM along with the ISO standards. Further various categories of techniques and applications are also explained along with the terminology which is important and needy to understand the concept of IAM. At last some case studies are explained along with the implementation components of IAM for e-healthcare system.

References

- [1] Broderick JS. ISMS, security standards and security regulations: information security technical report. 2006;11(1):26–31.
- [2] Humphreys E. Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House; 2016.
- [3] Pardo C, Pino FJ, and Garcia F. Towards an integrated management system (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards. *International Journal of Software Engineering and Its Applications*. 2016; 10(9):217–230.
- [4] Cremers C, and Horvat M. Improving the ISO/IEC 11770 standard for key management techniques. *International Journal of Information Security*. 2016;15(6):659–673.
- [5] Janis JA, Conklin DD, and Young RA. Access authentication and/or item process management using identification codes. Google Patents; 2018. US Patent 9,984,356.
- [6] Raspotnig C, and Opdahl A. Comparing risk identification techniques for safety and security requirements. *Journal of Systems and Software*. 2013; 86(4):1124–1151.
- [7] Sharma VS, and Trivedi KS. Architecture based analysis of performance, reliability and security of software systems. In: *Proceedings of the 5th International Workshop on Software and Performance*. ACM; 2005. p. 217–227.
- [8] Neubauer T, Klemen M, and Biffl S. Business process-based valuation of IT-security. vol. 30. ACM; 2005.
- [9] Sun HM. An efficient remote use authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*. 2000;46(4):958–961.
- [10] Melnikov A, and Zeilenga K. Simple authentication and security layer (SASL); 2006.
- [11] Xia F, Yang LT, Wang L, *et al.* Internet of things. *International Journal of Communication Systems*. 2012;25(9):1101.
- [12] Lamport L. Password authentication with insecure communication. *Communications of the ACM*. 1981;24(11):770–772.
- [13] Li X, Ma J, Wang W, *et al.* A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. *Mathematical and Computer Modelling*. 2013;58(1):85–95.
- [14] Chen BL, Kuo WC, and Wu LC. Robust smart-card-based remote user password authentication scheme. *International Journal of Communication Systems*. 2014;27(2):377–389.
- [15] Chen BL, Kuo WC, and Wu LC. A secure password-based remote user authentication scheme without smart cards. *Information Technology and Control*. 2012;41(1):53–59.
- [16] Lee WB, and Chang CC. User identification and key distribution maintaining anonymity for distributed computer networks. *Computer Systems Science & Engineering*. 2000;15(4):211–214.

- [17] Liao YP, and Wang SS. A secure dynamic ID based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*. 2009;31(1):24–29.
- [18] Kocher P, Jaffe J, and Jun B. Differential power analysis. In: *Annual International Cryptology Conference*. Springer; 1999. p. 388–397.
- [19] Messerges TS, Dabbish EA, and Sloan RH. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*. 2002;51(5):541–552.
- [20] Lee CC, Lin TH, and Chang RX. A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards. *Expert Systems with Applications*. 2011;38(11):13863–13870.
- [21] Truong TT, Tran MT, and Duong AD. Robust secure dynamic ID based remote user authentication scheme for multi-server environment. In: *International Conference on Computational Science and Its Applications*. Springer; 2013. p. 502–515.
- [22] Truong TT, Tran MT, and Duong AD. Modified dynamic ID-based user authentication scheme resisting smart-card-theft attack. *Applied Mathematics & Information Sciences*. 2014;8(3):967.
- [23] Leu JS, and Hsieh WB. Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards. *IET Information Security*. 2013;8(2):104–113.
- [24] Li X, Xiong Y, Ma J, *et al*. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. *Journal of Network and Computer Applications*. 2012;35(2):763–769.
- [25] Xue K, Hong P, and Ma C. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. *Journal of Computer and System Sciences*. 2014;80(1):195–206.
- [26] Gaharana S, and Anand D. Dynamic Id based remote user authentication in multi server environment using smart cards: a review. In: *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*. IEEE; 2015. p. 1081–1084.
- [27] Leu JS, and Hsieh WB. Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards. *IET Information Security*. 2014;8(2):104–113.
- [28] Das ML, Saxena A, and Gulati VP. A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*. 2004;50(2):629–631.
- [29] Giroux D, and Sharko J. Information security architecture for encrypting documents for remote access while maintaining access control. Google Patents; 2005. US Patent 6,978,376.
- [30] Sameshima Y, and Kirstein P. Authorization with security attributes and privilege delegation: access control beyond the ACL. *Computer Communications*. 1997;20(5):376–384.

- [31] Olden EM. Security and access management system for web-enabled and non-web-enabled applications and content on a computer network. Google Patents; 2002. US Patent 6,460,141.
- [32] Sharma DH, Dhote C, and Potey MM. Identity and access management as security-as-a-service from clouds. *Procedia Computer Science*. 2016;79:170–174.
- [33] Martin D, Grimes D, Warnock T, *et al*. Methods and systems for managing a virtual data center with embedded roles based access control. Google Patents; 2014. US Patent 8,806,486.
- [34] Fremantle P, Aziz B, Kopecký J, *et al*. Federated identity and access management for the internet of things. In: 2014 International Workshop on Secure Internet of Things (SIoT). IEEE; 2014. p. 10–17.
- [35] Sumra IA, Hasbullah HB, and AbManan JIB. Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In: *Vehicular Ad-Hoc Networks for Smart Cities*. Springer; 2015. p. 51–61.
- [36] Barbeau M, Hall J, and Kranakis E. Detecting impersonation attacks in future wireless and mobile networks. In: *Secure Mobile Ad-hoc Networks and Sensors*. Springer; 2006. p. 80–95.
- [37] Dojen R, Jurecut A, Coffey T, *et al*. On Establishing and Fixing a Parallel Session Attack in a Security Protocol. In: IDC. Springer; 2008. p. 239–244.
- [38] Gong L. Optimal authentication protocols resistant to password guessing attacks. In: *Eighth IEEE Proceedings on Computer Security Foundations Workshop*, 1995. IEEE; 1995. p. 24–29.
- [39] Albert R, Edgett J, and Sunder S. Method and system for identifying a replay attack by an access device to a computer system. Google Patents; 2002. US Patent App. 10/118,406.
- [40] Tang H, Liu X, and Jiang L. A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance. *IJ Network Security*. 2013;15(6):446–454.
- [41] Chen CM, and Ku WC. Stolen-verifier attack on two new strong-password authentication protocols. *IEICE Transactions on Communications*. 2002; 85(11):2519–2521.
- [42] Ku WC, Lee HL, and Chen CM. Reflection attack on a generalized key agreement and password authentication protocol. *IEICE Transactions on Communications*. 2004;87(5):1386–1388.
- [43] Chang YF, and Chang CC. Authentication schemes with no verification table. *Applied Mathematics and Computation*. 2005;167(2):820–832.
- [44] Katz J, Ostrovsky R, and Yung M. Forward secrecy in password-only key exchange protocols. In: SCN. Vol. 2. Springer; 2002. p. 29–44.
- [45] Mishra D, Chaturvedi A, and Mukhopadhyay S. Design of a lightweight two-factor authentication scheme with smart card revocation. *Journal of Information Security and Applications*. 2015;23:44–53.
- [46] Kumari A, Tanwar S, Tyagi S, and Kumar N. Fog computing for Healthcare 4.0 environment: opportunities and challenges”. *Computers & Electrical Engineering*. 2018;72:1–13.

- [47] Elhoseny M, Ramirez-González G, Abu-Elnasr OM, *et al.* Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access*. 2018;6:20596–20608.
- [48] Rahmani AM, Thanigaivelan NK, Gia TN, *et al.* Smart e-health gateway: bringing intelligence to internet-of-things based ubiquitous healthcare systems. In: *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE; 2015. p. 826–834.

Chapter 5

Application design for privacy and security in healthcare

*Arjun Khara¹, Dharmesh Singh¹, and
Deepak Kumar Sharma¹*

Electronic health records (EHRs) were seen as a panacea for managing all medical-related data about the patient. The goal was to identify the siloed data fragmented across various healthcare providers and combine it in a uniform way in order to provide the best possible diagnostics and make it easy for the practitioners to gather and study patient's medical data. However, despite decades into development, such record systems are still long ways off in terms of practical implementation. They have been dogged by various shortcomings and above all concerns regarding potential loopholes in the privacy and security of patient data. Given the poor track record of the industry when it comes to preventing illicit access and sharing of data, there is an ever-growing impetus to stanch the consistent violation of the privacy of an individual's personal information by illegitimate parties. In this chapter, we aim to develop an understanding of an EHR system, identify associated shortcomings, and the requirements that it is supposed to fulfil. We also present various proposed implementations that show promise in the development of a safe, secure, and unified EHR system. In the last section, we discuss the potential of blockchains and how they have the goods to deliver a perfect EHR system.

5.1 Introduction

Technology-driven solutions have revolutionized a large number of industries in unimaginable ways, paving the path towards more efficient processes with improved utilities and unique benefits. The healthcare industry has been at the forefront of this wave of adoption when it comes to equipment involving patient diagnosis and treatment. However, a crucial segment of this industry which involves maintaining patient records is still in the midst of a long-drawn overhaul process. Prior to this wave of digitization, the records of the patients were

¹Department of Information Technology, Netaji Subhas University of Technology (formerly Netaji Subhas Institute of Technology), Delhi, India

maintained through paper trails consisting of medical records and diagnostic reports. This meant that the patient had to be responsible for preserving these records and present them to the medical practitioners in case the need arose. This was highly inefficient and often would result in partial diagnosis due to the lack of availability of relevant reports. Moreover, maintaining such records on paper and ensuring their security and privacy is difficult. In order to tackle this, electronic medical records (EMRs) were introduced. The aim was to capture medical reports in a digital form hence making their storage and transmission easier. It also allowed patient data to be tracked over time hence improving the overall quality of healthcare. However, these implementations suffered from lack of organization. Each medical service provider maintains its own set of records for the patients it serves. Hence the information is siloed, and the relevant medical data have to be asked for when required instead of the instant availability that could have been delivered.

EHRs were designed with the purpose of solving all these problems. The end objective of these records was to act as a single nodal repository for every medical data related to a patient. This meant that (1) patient records would be accurate and up-to-date; (2) the access to information would be quick and efficient allowing for coordinated services; (3) there would be a general overall improvement in aspects of privacy as well as security of medical data; and (4) a significant reduction in costs as paper and other systems are replaced whilst also improving safety and reliability. The real-world implementations, however, have often run into various kind of issues. Though the proposals advocating the use of these records were made more than a decade ago, the industry is still in the middle of transitioning to such systems. This chapter aims to develop an insight into the key functionalities that are required to make a unified EHR system while also ensuring maximum privacy and security, as well as discuss implementations for the same. The first section develops an understanding regarding EHR, establishing its purpose, use case, structure, and requirements from systems implementing these. The follow-up section considers the particular aspects of privacy and security of such systems and the methods employed to deal with them. It also delves into proposals for cloud-based unified EHR systems. The fourth section provides novel solutions that are being proposed through the use of decentralized ledgers to tackle the challenges presented by current legacy systems. Finally, in the concluding section, we present the key points discussed in this chapter and the challenges to be overcome for future deployments.

5.2 Understanding EHR systems

Current implementations of EHR have come a long way since their inception, as a result of which the demands and associated problems have also evolved with time. EHR systems have suffered from the lack of a definite structure or functionality. It is more appropriate to define such records and systems as implementations of specific rules and requirements dictated by the standards. In this section, we will

review [1] the purpose of EHR, define its structure, and the actors that are a part of the EHR ecosystem. Finally, we shall list the requirements that an EHR system is supposed to fulfil.

5.2.1 What is an electronic health record

In order to develop an understanding of a health record system, a distinction needs to be established between an electronic medical record (EMR) and EHR. EMRs are simply a digital version of the paper-based reports generated by the healthcare provider. These are created, used, and maintained by healthcare providers to manage and monitor patient-related information. An EMR consists of a patient's medical records from the point of view of a single practitioner.

On the other hand, an EHR should be considered as a combined collection of EMR records maintained by various healthcare service providers with respect to a patient. The International Organization for Standardization (ISO) has defined an EHR [2] as a digital nodal collection of all reports and medical data concerning a patient. The records should preserve all historic, current, and future medical information concerning a patient. The standard states that the storage and exchange should be secure and privacy preserving. It should be accessible by various users only after proper authentication and authorization. The aim of such a system is to provide quality integrated healthcare and improve overall efficiency and reliability.

The issue with this definition is that it provides a very vague description of the data that EHRs are supposed to maintain. The literature regarding this is varied and perceptive according to the given use case and scenario. A patient's record can include previous medical history, medications, test reports, any complications, diagnosis, or active problems. However, this is by no means an exhaustive list and is often dependent on the context of use. The use case of such records is not just limited to planning and documenting patient care. It plays a significant role in the decision-making process related to both patient care and in the management of health policy. Moreover, the data collected by these records prove to be invaluable in clinical research and for imparting accurate medical services. Hence EHR also needs to take this aspect into account.

5.2.2 Structure of electronic health record

The key data components that are stored in EHR can be broadly categorized as diagnoses, lifestyle, records of existing medical history, referrals, treatment, present complaint (e.g., symptoms), tests, for example, radiology and laboratory, physical examination, and medication procedures. The structure of these records plays a crucial role in dictating the relative ease and efficiency in accessing the information. The classification centers around three categories namely, source-oriented, time-oriented, and problem-oriented [3]. Time-oriented records store the data as a function of time, and hence all the information is stored in chronological order. Source-oriented records organize information according to the context of information generation, for example, diagnostic reports, blood tests, visiting reports, etc. Each section arranges the information in a time-oriented manner.

Problem-oriented records are more rigorous in the filtering of information, wherein each problem is classified according to subjective information, objective information, assessments, and plan (SOAP) for a given patient. An EHR also stores unstructured free text alongside digital data. The standard used in the records which include vocabularies, nomenclatures, and classifications dictates key aspects when considering data exchange and interoperability. Attempts have been made to develop standardized methods of organizing and storing data, such as modified versions of Norton scale [4] and information collections based on daily activities, skills, behavior, nursing care needs, and daily living score [5].

5.2.3 Actors in an electronic health record system

Developing a structure for the records requires to consider the entities that shall be participating in the generation, access, and retrieval of data. A general classification involves splitting healthcare services into three categories, that is, primary, secondary, and tertiary. Primary healthcare consists of services provided by practitioners. Secondary care is provided by specialists, usually after a reference from a primary care service. Tertiary care consists of specialists working for hospitals [6]. EHR data are used both by administrative staff and healthcare professionals, such as laboratory technicians, radiographers, nurses, pharmacists, physicians, and radiologists as well as the patient and related family members. This presents a challenge for EHR systems as it must provide a single view of information about the patient to all these actors while also making sure the aspects of privacy and security are followed. In addition, there are also requirements from pharmaceutical industries and medical research institutes for access to medical data for research purposes. Government institutes might also require access for development of healthcare related and other policies regarding the national interest.

5.2.4 Requirements from an electronic health system

5.2.4.1 Standardize structure of data, vocabulary, and nomenclature of these systems

The EHR systems need to have a definite set of standards for dictating the structure and nomenclature of the data being stored in such systems. This is the first and foremost step in the formation of a unified EHR, as semantic uniformity is required for data exchange. The requirement of data standardization is a must for construction of interoperable systems. Current systems usually work by aggregating data from various EMRs concerning a patient, and nonuniform standards make it harder for this to happen.

5.2.4.2 Interoperability and open systems

After the establishment of structured data and terminologies, the next key requirement is to provide standards for interoperability. The establishment of standardized rules for data exchange is a necessity for communication between various EHR implementations. In order to achieve this, standardized models such as openEHR [7] and HL7 Clinical Document Architecture (CDA) [8] are under

development. OpenEHR is based on a two-level model. The first level is the only one implemented and it vastly reduces the dependency on variable content definitions. The second level is composed of formal definitions of clinical content in the form of archetypes and templates. This two-model approach has the added benefit of being compact. In addition, it is more manageable than single-level systems. The systems are built to consume archetypes and templates as they are developed into the future. The use of archotyping allows for new relationships between information and models, as depicted in Figure 5.1.

The HL7 V3 standard is based on a model-driven methodology. The models are based on the reference information model (RIM) [9] and depict the static and behavioral aspects of the standard. RIM represents a static model of healthcare workflows. Its structure is both flexible and extensible. Clinical document architecture (CDA), which is based on XML, is an electronic standard used for clinical document exchange. It is used for defining the semantics and detailed structure of medical documents.

5.2.4.3 Increased patient control

In the healthcare industry, the service providers are the creators of the data, however, the patients are the owners of their medical data. Ensuring transparency in ownership of EMRs is much harder than physical paper reports which were handed over to the patient. The data persist in the form of EMR in the systems of the

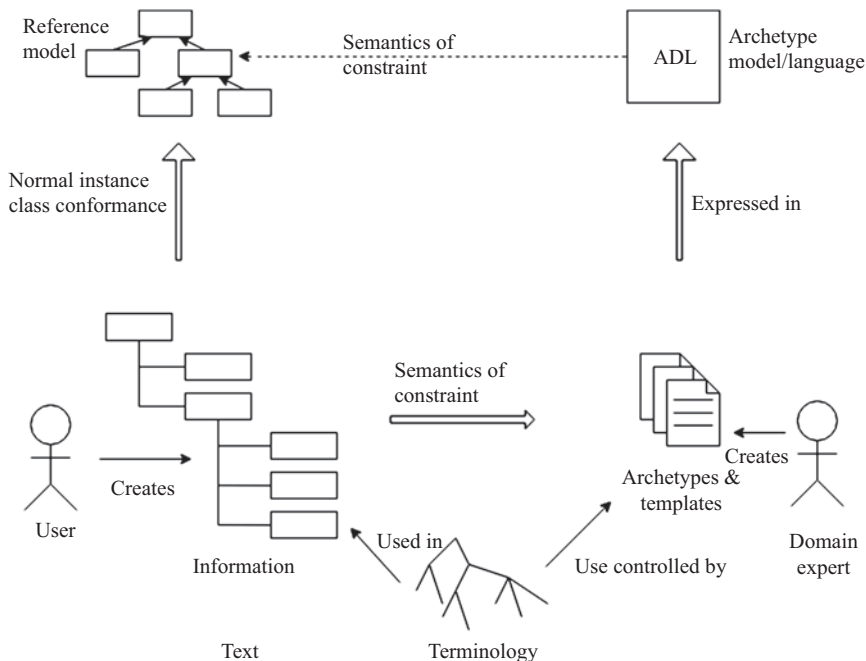


Figure 5.1 Archetype meta-architecture used in OpenEHR [7]

service providers. The patients usually outsourced the storage and management of their digital health records to third-party solutions. In either case, ensuring the security and privacy of these records is of utmost importance. Given the fact that patients are the owners of their own medical data, any form of information sharing should be done only after it has been consented by the patient. The key issue is that the patient data are dispersed and hence unifying this fractured data presents a formidable challenge. Patient-centric systems will allow for patients to be in full control of their own medical data. They will have full control on the collection, storage, and usage of their medical information made possible by the merging of EHR from a variety of systems. The development of cloud-based personal health systems such as Microsoft HealthVault or Google Health presents a viable option. Cloud-based personal health systems will be further discussed in Section 5.4.3.

5.2.4.4 Privacy and security

The challenges concerning current systems are in large parts related to lack of coordination and a single viewpoint when it comes to standardization [10]. Medical information of a patient is extremely confidential. Hence a key factor dictating the formation of these record defining standards is the promise to ensure that the stored information is completely secure and is accessible only by authorized entities. It is on the foundation of these promises that current systems are built on. Presence of a security exploit can present a major impediment in their deployment as well as raise serious concerns in the community regarding the safety of digital record systems.

Security of a system is defined along three broad paradigms [11], namely confidentiality, integrity, and availability (CIA). Confidentiality is defined by ISO EN 13606 standard [12] as the ability to hide information from unauthorized people or in other words, the information is accessible only to those who have the necessary authorization. Integrity involves ensuring that the data have not been modified by unauthorized entities and are an accurate representation of the original. It ensures that the information has not been tampered by any malicious actors. An extension of integrity also involves ensuring auditable records of information, hence incorporating accountability. Availability ensures that the information is accessible at any point in time by authorized entities. This is extremely important to ensure that the system is resistant to extreme circumstances such as natural disasters, or specifically engineered attacks such as distributed denial of service (DDoS). Privacy involves ensuring that the data are protected from unauthorized access and that a third party gets access to only the minimum required information for processing and nothing more. It requires giving owners the control to determine access and distribution of their personal information [13].

Designing a system that fulfils these requirements proves to be extremely challenging given a large number of gray areas. For example, how to access the records in case of an emergency, how to define access control and who defines it, how to make trade-offs between efficiency and complete security. Healthcare systems have fallen victims to hacking attempts [14], often leading to identity thefts on a large scale. There have been more than 900 major security breaches post-2014

resulting in exposure/theft of more than 135,060,443 healthcare records. The records are also susceptible to misuse by organizations seeking to make a profit from that data, such as cases of buying and selling a doctors' prescribing habits to pharmaceutical companies. World Privacy Forum has warned that storing sensitive data on third-party servers is vulnerable to blind subpoena or change in user agreements. In light of these breaches, it is the need of the hour to develop applications that are built around security and privacy as core principles rather than as an added requirement. In conclusion to these definitions, an EHR system needs to ensure the following requirements [15]:

1. **Compliance with standards:** Ensuring that the models and implementations work within the framework of the defined standards.
2. **Information systems acquisitions, development, and maintenance:** Ensuring, that new devices and infrastructure is either developed or acquired and subsequently maintained.
3. **Access control:** Ensuring that only the authorized users are able to access and control the data.
4. **Communications and operations management:** Providing clear operations oversight and nonambiguous interpretation of data.
5. **Availability:** Ensuring that the information is accessible at all times without any downtime.

5.3 Solutions for EHR development

In section 5.2, we developed an understanding of an EHR system and also presented the requirements that it is supposed to fulfil. In this section, we will first discuss various methods that are employed in EHR systems to achieve privacy and security. This will be followed by some system frameworks that combine these implementations to build a secure and privacy preserving EHR system.

5.3.1 Compliance

Standards and regulations summarize key principles and practices for ensuring privacy and security. They help an organization reduce costs, improve efficiency in development, and deployment as well as ensure risk avoidance. The most frequently cited regulation is the Health Insurance Portability and Accountability Act (HIPAA) that dictates the regulations within the United States. HIPAA was designed to lay the guidelines for handling of medical information by the healthcare service providers as well as streamline the flow information in the healthcare industry. It ensures that the patients have access to their medical records and also control over how their data are shared. HIPAA also has a minimal disclosure principle stating that only the required amount of data should be shared to any third party and nothing more. Europe has its own standard, the CEN/ISO EN 13606-Part IV. However, this standard is yet to witness widespread adoption given that it's still relatively new. There are a number of other standards, though none of them is widely adopted. The lack of (1) a harmonized policy on trust, privacy, and

confidentiality and (2) common security standards acts as a barrier for secure inner and cross organizational communication. This again presents a challenge for authorities to work together and propose a unified standard or regulation that transcends the regional barriers, similar to other global ISO standards.

5.3.2 *Encryption techniques*

EHR systems have a choice on whether to store the information in the servers in an unencrypted or encrypted form. However, it is advocated that in order to maintain confidentiality, data integrity and privacy, the information should be stored in an encrypted form. There are two options for data encryption, that is, symmetric and asymmetric schemes. The problem with asymmetric cryptography is that it is extremely inefficient, especially in cases of health records concerning imaging data. Moreover, they have inherent privacy weaknesses when searchability or hidden labels are required [16]. Hence, for the purposes of efficiency, the use of symmetric cryptography is preferred wherever possible. One solution is to use a hybrid public key infrastructure (HPKI) proposed by Hu *et al.* [17]. The infrastructure is HIPAA compliant. It employs public key infrastructure for sensitive but computationally nonintensive data and the more efficient symmetric scheme for data involving image data. Still, encryption on medical data involving images is computationally expensive and time-consuming and requires more work. Efforts are being made to tackle this issue. Kanso and Ghebleh [18] proposed a solution which uses a full and selective chaos-based image encryption scheme. The method uses several rounds, consisting of two phases each, that is, masking and shuffling phase. The use of a pseudorandom matrix makes the scheme efficient as well as maintains security. Some biometric solutions also provide promising results in the field of encryption [19,20].

The servers responsible for storing the encryption keys are also susceptible to breaches. One method is to maintain separate servers for data and key storage so that the keys are not compromised in the event of a breach in the data servers. The other is to completely eliminate key storage in servers by allowing patients to create and maintain their own keys. Such methods will be discussed in patient-centric EHR systems presented in Section 5.4.3. There are other forms of encryption techniques that provide access control, such as identity-based encryption which will be discussed in Section 5.3.4. For secure transport of information over the Internet, the industry standard encryption techniques such as transport layer security (TLS) is used, thus preventing data spoofing or man in the middle attacks.

5.3.3 *Access control*

Dealing with authorization and access control presents the most formidable challenge in the development of EHR systems. It requires ensuring that the information of the records is never visible, accessible, or modifiable by unauthorized actors. There are two broad ways to approach this problem. The first involves storing the records in centralized servers under the protection of the party managing the databases. Access control methods are used to provide a fine-grain level of access

and authorization in such cases. These methods usually store information in an unencrypted format as the access control acts as a firewall and protects the system from any unauthorized access. The other alternative is to merge the encryption of information along with access controls. It ensures authorized access and integrity of data, hence providing both security and privacy as the data are stored in an encrypted format. This is made possible by employing the use of Cryptographic Access Control Model. This also opens avenues for constructing composite EHRs consisting of information from multiple independent sources. This section provides an overview of the former class of access control methods.

An identity management system is typically composed of three major elements: users, systems/applications, and policies. The access control policy dictates the interactions of users with the system. It is typically based on the privilege and right of each practitioner authorized by the patient or a trusted third party. There are two widely used implementations of access control models, namely role-based access control (RBAC) [21] and attribute-based access control (ABAC) [22,23]. The following subsections provide an overview of both the models. In addition to both of these, we also discuss the cryptographic access control model.

5.3.3.1 Role-based access control

RBAC works by defining a class of roles and access levels, providing a control mechanism that is policy neutral. RBAC finds extensive in dynamic environments which constant changes to permission levels by assigning access based on the roles and assigned tasks rather than a specific subject. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments and makes RBAC extremely suitable for access control in commercial and government organizations. RBAC functions on a minimal data disclosure policy, that is, only the relevant information which is required by personnel to fulfil one's role are given access to. The distribution of access controls can be based on factors such as responsibility and authority. RBAC can also limit access to computer resources, such as the ability to create, view, or modify files.

5.3.3.2 Attribute-based access control

ABAC is the most refined access control model and can be used to provide extremely fine-grained control over the access policies. ABAC works by defining attributes, broadly of three types, that is, user attributes, attributes associated with the system to be accessed, and current environmental conditions. The access policy works by combining these attributes together. While RBAC requires a predefined set of roles with associated privileges which the users are assigned to, ABAC, on the other hand, can develop complex Boolean rules combining the defined attributes providing more flexibility. A comparison between RBAC and ABAC is provided in Table 5.1.

5.3.3.3 Cryptographic access control

The drawback with RBAC and ABAC models is that they require a central authority referred to as a reference monitor for mediating access. This is fine for small systems, however, as systems scale, there is the requirement for these access

Table 5.1 Comparison of RBAC and ABAC access control models [24]

	RBAC	ABAC
Level of customization	Low	High
Levels of provided anonymity	Low	High
Total efficiency in execution	High	Low
Overall scalability	High	Low

protocols to function in a distributed manner. Distribution protocols in these schemes do not work well as these were designed with a central authority in mind. The aim of the cryptographic protocol [25] is to allow for a distributed access control paradigm. The objective is to replace the reference monitor and allow for the access control mechanism to function in an untrusted environment. It defines an implicit control mechanism. Cryptography is used to provide integrity and confidentiality of the data managed by the system. These schemes usually consist of partially ordered sets of security. Each class is representative of a group with a particular access level to a certain section of data. Identity-based encryption presents a class of such implementations and is discussed in Section 5.3.4. The main issue with this model is the requirement of a large number of keys, making key management a demanding task.

5.3.4 Identity-based encryption

As highlighted earlier, the problem with the above discussed methods is the requirement of a trusted server. The data are stored in plaintext and is prone to attacks and unintended disclosures in the event of server failures or insider attacks. Encrypting the data prevents such attacks. Traditional public key cryptography works on the concept of encrypting information for a specific receiver given their public key. This requires the functioning of a public key infrastructure to provide the sender with a public key certificate for verifying the authenticity of the association of a public key to a specific receiver. This problem can be solved by maintaining a central server which stores the public keys mapped to entities. However, public-key cryptography works on complete data encryption, that is, there is no way of providing access to a restricted group apart from encrypting the information for each user separately. Hence, such a system would involve the use of a separate access control mechanism, such as the ones proposed in Section 5.3.3. The introduction of identity-based encryption [26] (IBE) changed the traditional public key cryptography system by allowing for encryption along with access control. Also, the public key could consist of an arbitrary string, for example, the email address of the receiver. Here we discuss the two most widely used implementations of IBE scheme.

5.3.4.1 Ciphertext policy attribute-based encryption

Sahai and Waters [27] introduced Fuzzy identity-based encryption and is also known as ciphertext policy attribute-based encryption (CP-ABE). The data are

broken down into a set of attributes, that is the keys, as well as identities are considered as a set of descriptive attributes. It is within this universe of attributes defined for the system, that the access policy is drafted. Decryption by a given user will be successful only if the users key and the encryption key are within a defined distance metric. In other words, decryption by a user will be possible provided that his attributes fall within the policy of the ciphertext in question.

The policy could be defined over attributes in the form of conjunctions, disjunctions or (k, n) threshold gates requiring at-least k attributes to overlap between the ciphertext and the private key. The system, therefore, allows for a certain amount of error-tolerance and hence is extremely suitable for use in biometric identifications. The system is also resistant to collusion attacks. For instance, given a system with ciphertext defined over attributes $\{A, B, C, D\}$, and two users with private key attribute sets as $\{A, C\}$ $\{B\}$, respectively. If the policy for the ciphertext were given as $\{(A \text{ and } B) \text{ or } D\}$, then collusion by both the users would still not decrypt the ciphertext. Implicit authorization makes CP-ABE an attractive option, as both encryption and access control schemes are merged. Moreover, the users can obtain their private keys even after the data have been encrypted with respect to the defined policies.

5.3.4.2 Key policy attribute-based encryption

The main issue with CP-ABE is that its design was more suitable for biometric applications with the objective of functioning within the defined error tolerance. However, its application for controlling access to data are limited. The threshold gate is the only supported access structure and the threshold is fixed at the setup time. Key policy attribute-based encryption (KP-ABE) [28] allows for a much finer level of access and control. Unlike CP-ABE, key policy cryptosystem labels the ciphertext with a set of descriptive attributes instead of the private key. Access trees are constructed and hence bound to every private key such that the leaves act as attributes and interior nodes as threshold gates. The decryption of the ciphertext can be successful only if there is an assignment of attributes from the ciphertext to nodes of the tree such that the tree is satisfied. This scheme is similar to the secret sharing scheme [29] except the fact that secret sharing scheme allows for the cooperation of different parties, whereas this is not the case in KP-ABE. Apart from the fine-grained access control provided, another advantage of this cryptosystem is that there is provisioning for hierarchical access control. A private key can be derived from another private key given the derived key is strictly restrictive to the original one.

5.3.5 Key management

In order to support encryption mechanisms, management of keys is extremely crucial. There are a number of characteristics that a key management system should exhibit, that is, (1) the number of keys that need to handle should not be large. It becomes tedious to manage a large set of keys as the number of relationships increases with time; (2) keys should be easy to maintain and store; (3) keys should not contain any private information; (4) keys should be revocable; and (5) keys

should be traceable so that they can be revoked when a user leaves a group. There are number of key management systems in use today; however, for EHR use cases, hierarchical key management is a suitable candidate.

Hierarchical access control systems work by partitioning users into multiple classes. These classes are organized by hierarchy and are known as security classes. The hierarchies in the system are based on the division of privileges. A security class inherits the privileges of its descendant classes. The main problem faced in said system is the assignment of keys. The distribution and assignment of keys to users and resources need to be done correctly in order to enforce the access rights. There are three dictating factors, how many keys does a user own, computation the user performs, and amount of resources required by the server. The aim is to minimize all three. Another augmentation to this system is the introduction of time-based access control wherein the access is time controlled. Crampton *et al.* [30] provide a categorization of key management in hierarchical access control. The first provable secure solution using time-based hierarchical scheme is given by Ateniese *et al.* [31]. It is secure against both achieving pseudo-random keys and key recovery. The use of hierarchical keys is discussed in Section 5.4.3 in the patient-centric model proposed by Benolah *et al.* [16]. An alternative proposal involving CP-ABE is used by Narayan *et al.* [32] that requires a single root key, though the model is not completely patient centric as there is the need of a trusted authority to maintain a repository of public keys.

5.3.6 *Digital signature and verification*

Digital signature schemes are extremely important for providing nonrepudiation, integrity, and authenticity of digital documents. Zhang *et al.* [24] propagate the use of anonymous signatures. We shall be discussing two signature techniques of significance in EHR systems, namely (1) anonymous signatures and (2) threshold signatures.

5.3.6.1 **Anonymous signatures**

In order to keep the identity of the user anonymous and ensure privacy, techniques for producing pseudonym identifiers are employed. However, anonymous signatures guarantee anonymity in the signature scheme itself. There are a number of schemes for producing anonymous signatures, we shall be looking into the two most important ones: (1) group signature and (2) ring signature.

Group signature: It was introduced by Chaum and Van Hejst [33]. The scheme revolves around a group of members managed by a group manager. It allows for a member of the group to anonymously sign a message on behalf of the group members. The task of the group manager is to initialize the group and also handle member joining and revocation procedures. In addition, the group manager can also deanonymize a signature in the case of a dispute. Every member of the group has a separate private signing key, and a single group public key. This group public key can be used by any third party to verify whether a signature has been signed by the group or not.

Any group member can sign on behalf of the group, and it will not reveal the identity of the signer. Each member of the group should have a long-term identity tied to the group and to the members private key. The relationship, however, is known only know to the group manager.

Ring signature: It was developed by Tauman, Rivest, and Shamir [34] as a way to leak secret information without actually revealing who signed the message. The objective of the scheme is similar to that of the group signature scheme, that is, preserve the anonymity of the signer behind a group. A verifier can check the validity of the signature without knowing who generated it among all possible ring members. Moreover, two signatures generated by the same signer are unlink able. There are two key difference between ring and group signature schemes. The first that there is no facility to revoke a signature in ring signature scheme. The second that there is no need to set up a group in ring signature scheme, that is, any group of users can act as a group for a scheme without any prior prerequisites.

5.3.6.2 Threshold signatures

Threshold scheme [35] requires, that for a given system having n participants, in order to sign or decrypt a message, there needs to be cooperation amongst at-least t members. In other words, threshold signature is a special way of doing multiple signatures, where for a given group of participants, some minimum number of them have to contribute a share of the signature in order to produce a single overall valid signature. The group has a public-private key pair, wherein the private key is shared amongst the participants. Shamir's secret sharing scheme is also a threshold scheme. It allows the user to take a secret and create a set of secret shares from it. A secret share does not leak any information about the original secret and thus is useless on its own. Boneh, Lynn, and Shacham (BLS) [36] scheme, using an extension of Shamir's secret sharing, allows for the process of key generation needed for producing keys used for signing and verifying messages to be done in a distributed way thus eliminating the need for a single participant to be trusted. This is a very powerful notion, as it means the original secret never has to be never observed again. Once the shares are divided, you can simply divide these secret shares in multiple places. These secret shares can produce their own signatures, but they only validate against their public key. However, if we are able to collect m out of n of these signature shares and perform polynomial interpolation which is carried out for secret shares, we will recover the signature that would have been created if the original key had been used.

5.4 EHR system framework

5.4.1 Advantages of cloud

The frameworks for EHR systems are witnessing a sea change with the advent of cloud computing due to the significant advantages that it presents over current systems. The objective of an EHR system was centered around unifying the EMRs

in use by healthcare service providers. The idea was that vendors would develop systems that would provide an EHR for patient data spanning multiple healthcare providers and consist of a single view. The reason why these EHR systems were never able to fulfil their objective was that this concept of a single view was not based on a single implementation, but on the basis of interoperability. The frameworks were based on a simple client–server model. This meant that the clients would have to deploy their own servers to run the EHR system. Hence the only way to unify the patient records was through a network that supported robust data exchange and interoperability between different client systems. The problems for the client did not end here, as deploying personal servers would require the client to go through a lot of trouble, such as setting up the necessary hardware, maintaining the database, ensuring database security and associated legal risk in case of breaches, and risk of faults and downtimes in case of failures amongst others. Moreover, the systems were still lacking in providing seamless interoperability.

The development of cloud-based systems provides a significant step forward in the development of EHR systems that satisfy all the requirements. There are a number of advantages that cloud-based solutions bring compared to the traditional model. Some of them being:

1. **Availability:** Cloud computing servers are distributed across multiple geographical regions which play an integral role in providing uninterrupted services and faster access and retrieval times.
2. **Fault tolerance:** These services are fault tolerant, which means the possibility of down times is extremely low. The data are replicated across multiple servers and the possibility of corruption or loss is extremely low as compared to the traditional client–server models.
3. **Charge per computation:** Traditional client–server models required a heavy initial investment in terms of both hardware and software commitments. The key advantage of cloud-based solutions is that it requires zero initial investment. The users have to simply pay according to the fee structure for the number of resources they use.
4. **Scalability and flexibility:** Resources can be dynamically provisioned and released based on the user's demand. This also means that they don't have to worry about how many resources are required at the beginning. They can scale the resources up and down according to their needs.
5. **Multicloud deployment:** In order to prevent monopoly, users can engage in multicloud deployment.
6. **Broad network access:** Users can connect to the cloud servers without any geographical restrictions and through any platform.

5.4.2 Organization of EHR frameworks

Therefore cloud-based solutions present a significant benefit in the development of new EHR systems that can possibly deal with existing problems and hence are the way forward for future systems. Taking these considerations into account,

healthcare service providers have the following options when it comes to deployment of EHR systems.

1. **Unencrypted data storage:** The medical records are stored in the servers in an unencrypted form. Access and authorization are performed through access control models that have been covered in Section 5.3.3. The problem with this approach is twofold. The first is regarding the security of the data. In the event of a server breach, the personal data of the patients will be compromised. The second revolves around the choice of trust in regard to deployment. If personal servers are used for deployment, then the patient has to trust the healthcare service provider for the fulfilment of security and privacy requirements. However, this comes with the downsides of the client–server paradigm discussed before. The other option is to outsource the storage of data to a third-party cloud provider. This again requires the establishment of trust that the third party will not violate any standards in regard to privacy.
2. **Encrypted data:** The first option is not fool proof when it comes to security and privacy aspects. Hence the solution is to store the data in an encrypted format. There are a number of ways of dealing with data encryption: (1) the extent of data encryption and (2) the handling of encryption keys.
 - a. The extent of encryption decides how much data are encrypted as well as its distinction from access control. The first method is to simply encrypt the data and then provide access control methods, similar to the ones discussed in unencrypted data storage. The second is to merge encryption and access control through novel encryption schemes such as identity-based encryptions discussed in Section 5.3.4.
 - b. The next requirement is the secure handling of encryption keys. If the keys are handled by third-party solutions, then we have the same requirements of trust as that in unencrypted data storage. The other option is the introduction of patient-based encryption schemes eliminating the need for a central server for key management.

Lastly, a relatively young but promising development is that of personal health record (PHR) systems. The aim of these is to fulfil the true purpose of EHRs, that is, a single medical record system for all purposes and which is truly in control by the patient's themselves. The framework for a successful PHR system will have to deal with the problems presented above along with the additional requirements of integration with existing EHR systems for smooth onboarding of data and users. In the following subsection, we shall dive into some proposed cloud-based EHR systems.

5.4.3 Cloud-based electronic record systems

The server models of cloud systems can be divided three broad categories [37], namely (1) Central Server Model; (2) Peer to Peer Server Model; and (3) Hybrid Server Model. Hybrid server models give a significant advantage over the other two. The framework presented by Gul *et al.* [38] is shown in Figure 5.2. It proposes

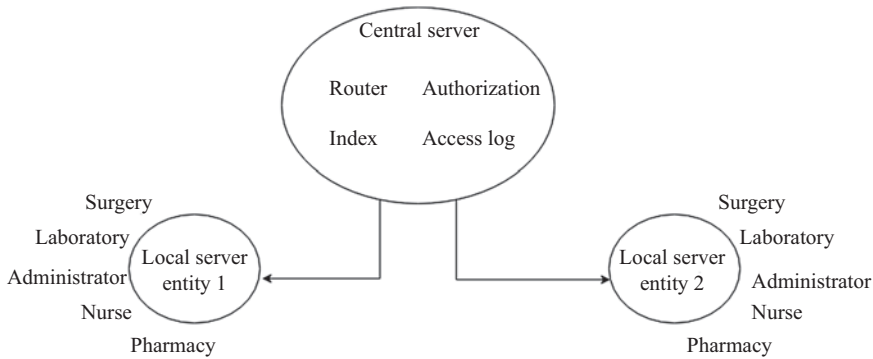


Figure 5.2 Cloud-based national EHR system [38]

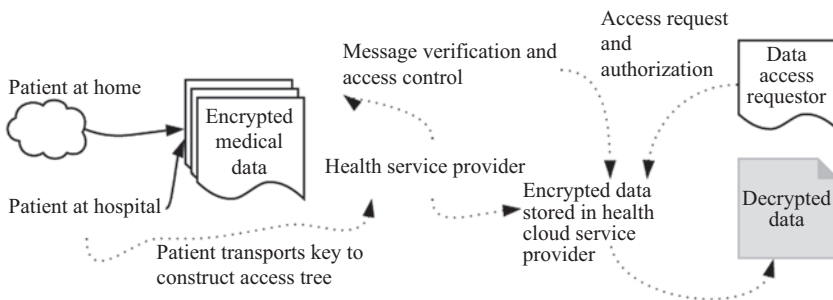


Figure 5.3 Patient-centric cloud-based EHR system by Barua *et al.* [42]

the use of a hybrid cloud model, with a community cloud acting as a central server. The framework proposes linking of separate databases of various healthcare providers to the central community cloud server.

However, the central server shall not store the records themselves. Instead, the model proposes maintaining an index of the unique location and health record identifiers, allowing for an EHR to be identified. The model also involves the use of routing service to forward messages to the correct locations, a temporary storage area and an access log for maintaining an audit of the requests made. The addition of any new EHR record to a local server is followed by the creation of a new record on the central server pointing to this EHR record. The system deals with patient queries by employing a unique patient identifier. This model provides a high-level overview and does not mention the specifics regarding associated security and privacy provisions.

Most of the proposed cloud-based EHR models state that the records stored in the cloud should be encrypted. Some implementations explore fog computing and use of biometrics [39–41]. In order to produce patient-centric EHR models, the use of identity-based encryption is widely used. Barua *et al.* [42] proposed a patient-centric PHR system. The proposed model, shown in Figure 5.3, uses cloud services

solely for data storage. The stored data are encrypted using ciphertext policy attribute-based encryption, providing both security and access control. The model states that Trusted Authorities, which will usually be authorized healthcare providers, will be responsible for issuing, revoking, and updating the keys. The access rights to users are granted based on their roles. The patient defines the access control policy, and the trusted authority constructs the respective access tree for the patient. These records are then transferred to the cloud storage provider.

The concept of a patient-centric EHR addresses the problems of privacy by allowing the patients to control their own medical information. Benolah *et al.* [16] designed a patient-centric model that employs hierarchical identity-based encryption (HIBE). The system supports partial access rights and searching over records. The patient's records need to be partitioned into a hierarchical structure. Each portion is encrypted using its own key. These keys can all be derived from a single secret key. This means that the patient can make separate decryption keys for various subsections of the records. These subsections hence can be shared to other third parties including medical service providers by providing them with the associated decryption key. An advantage of this hierarchical structure is that it can be extended to generate additional sections within a given subsection. As all the keys are controlled by the patients, there is no need for a third party to provide key storage and management facility, thus providing maximum security and privacy. This gives the flexibility of implementing the model over any third-party data storage solution. However, the system presents problems when it comes to key management. With an increase in access controls, managing a separate key for every subsection becomes cumbersome. Also, the hierarchy is fixed, meaning there is only one way to partition the record. There are also no facilities for key revocation and key recovery options.

A similar model by Narayan [32] also reduces the role of a cloud operator to data storage. The access control is also performed through the ciphertext policy-based attribute encryption model. Here the trusted authority is also responsible for maintaining a public directory required for publishing system public values and parameters needed for cryptographic operations. The keyword search facility has also been addressed. A patient's records can be searched based on a keyword by the healthcare provider without the cloud server knowing the keywords. The server would simply return the matched entries. The only vulnerability is the dependence on a trusted authority to issue keys. The main advantage of this system over Benolah *et al.* [16] is the relatively easier management of keys. The use of a patient's attributes to encrypt the data means that users require a single private key. In addition, the keyword search facility is more flexible, and patients are also given the facility to revoke the access to healthcare providers if needed.

Addressing integration of existing EHR records spread across multiple healthcare providers is still a sticking point. Zhang *et al.* [24] proposed an EHR reference model that would allow for the aggregation of EHR data from multiple providers by forming composite EHRs along with providing fine-grain access control. The model discusses a use case scenario involving group participation on a composite EHR, as shown in Figure 5.4. The aim is to first extract the necessary

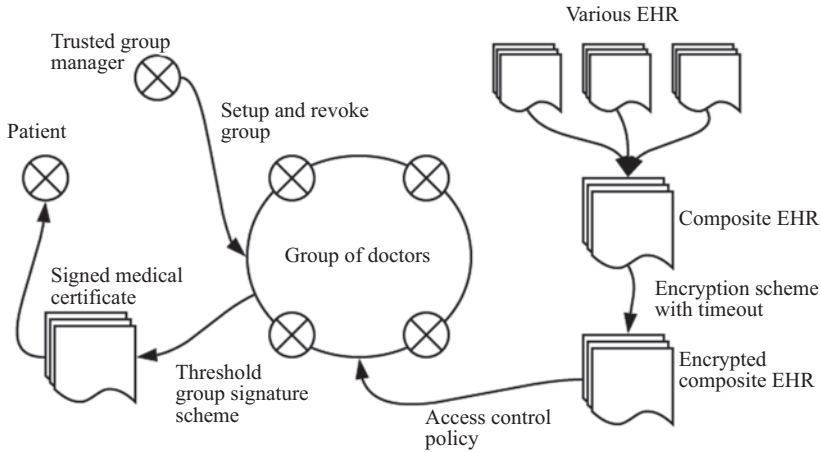


Figure 5.4 Forming a composite EHR from multiple sources [24]

details from a patient's EHR records which would be spread across multiple healthcare providers and combine them to form a composite EHR for the required purpose at hand. The second step is to establish the access control policy that would allow for a set of participants to access the data depending on their authorizations. The group would be managed by a group manager and all access control policies will be set by the patient. The third step concerns the scenario wherein the group proposes a treatment and the required document has to be digitally signed by the patient, which would ensure accountability and nonrepudiation in future. The system needs to make sure that the data should be distributed based on the HIPAA minimal disclosure principle and is also certifiable for its authenticity. The model is divided into three key portions: (1) secure EHR collection and integration, (2) secure storage and access management, and (3) secure usage. This workflow is shown in Figure 5.5.

Integration: This needs to fulfil two requirements: first that the EHR data being integrated is authentic and valid, and second on dealing with different EHR formats and deciding the format of the composite EHR. The model proposes uses of either attribute-based composite model or the role-based composite model. The attribute-based model has been discussed in Section 5.3.4. Even though it is highly suitable for providing fine-grained authorization and access control, the attached complexity and the significant increase in access times make the system cumbersome. An increase in the number of users and rules requires authorization for each and every node. This translates to a direct increase in the time taken to manage the system as well as data access and retrieval times. The other alternative is to use a role-based composite model. The proposed model assigns every patient an id (PID) and a corresponding token which is a hash value of the PID, serving as a pseudonym for privacy. This token is mapped to an EHR tree and serves as its root. The hierarchical structure of the tree can be based on a template, for example,

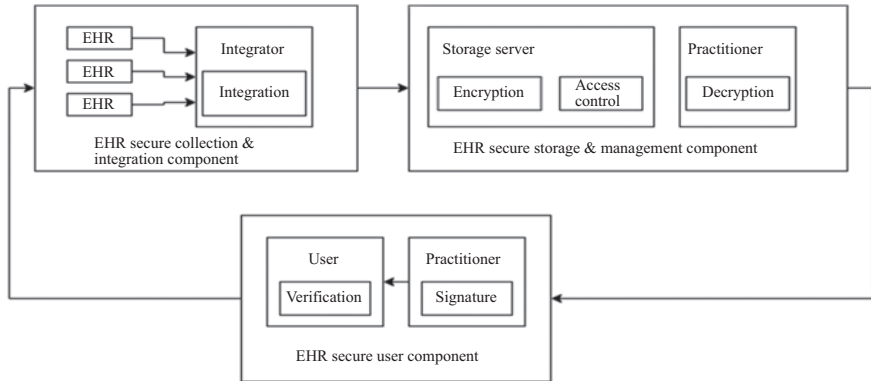


Figure 5.5 Dataflow in a composite EHR system [24]

Figure 5.6 consists of five levels. The first three levels are fixed, the root is always the patient token, followed by practitioners corresponding to various service providers and finally the specific id of the practitioner for that given service provider, similar to employee id. The nodes below these levels are related to the specific medical diagnoses or other reports. For faster and easier retrieval, the child nodes are ordered alphabetically from left to right. The practitioners are grouped by their roles in the first level.

Storage and usage: The authors leave the implementation specifics of this open-ended. Which means, the storage of the data could be floated to a third-party provider, and the choice of whether encryption should or should not be used for storage is left to the user. For applying access control, any of the three methods that were discussed in Section 5.3.3 could be deployed. However, the authors specifically state that in order to satisfy both fine-grained access control as well as security and privacy, the solution should be a conjunction of access control methods and security techniques. This supports the arguments presented earlier in Section 5.3.4 on providing access control through identity-based encryptions. For usage scenario, involving integrity and authenticity, any of the schemes discussed in Section 5.3.6 in can be implemented.

5.5 Blockchain for EHR systems

In the previous sections, we developed an understanding of the requirements and expectations that EHR systems are supposed to satisfy. To that end, we also reviewed various implementations that achieve the same. However, there are some core issues that these systems would never be able to solve as it stems from their concept of centralized architecture. In this section, we will first review some core problems that centralized architectures suffer from followed by the basics of decentralized ledgers and the associated advantages. Lastly, we will discuss some proposed implementations for blockchain-based EHR systems.

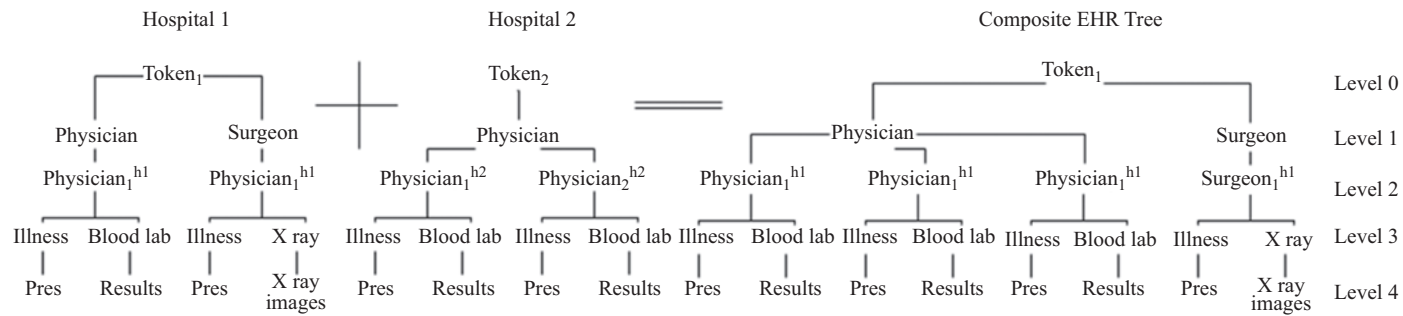


Figure 5.6 Access tree for role-based composite model [24]

5.5.1 Problems with centralized architectures

EHR was defined as a digital nodal collection of all reports and medical data concerning a patient spanning various service providers and providing a single view of all the patient information. The EHR implementations that we have studied till now require management by a trusted authority to run the system hence resulting in centralized trust-based architectures. There are some inherent issues with such implementations.

5.5.1.1 Interoperability and fragmentation

The core aim of the EHR system is to provide a single picture of patient information. The nearest that we have come to realize this goal is through the construction of cloud-based PHRs systems including a possible implementation involving the construction of composite EHRs managed by the patient which was discussed in Section 5.4.3. However, the key point to note here is that all these implementations are more or less similar to standards, and it is up to the vendors to decide on what to choose from and how to go about the implementation with the end goal being the same, which is conformance to the standards. The end result is that both the patients and consumers have a wide variety of software applications to choose from and all these implementations have to make sure that they allow for smooth data exchange and interoperable functionality.

This proves to be a grey area as data exchange is a necessity for the functioning of EHR systems and not only suffers from implementation problems due to non-uniform standards but also intended interfering with the flow of data. Moreover, they charge the customers unreasonable prices for the same [43]. The inability to share data in-turn gives rise to fragmentation of information, which is what the EHR systems were supposed to solve in the first place. This results in a catch 22 situation, as a solution would not become what a true EHR system aspires to be unless there is widespread adoption of that single implementation. This notion of trust in a single authority and the presence of multiple operators is the reason why centralized architectures are not suited for a unified EHR system. We shall see later, how decentralized solutions can solve these two core problems of centralized systems.

5.5.1.2 Security and privacy issues

Centralized systems also present problems when it comes to implementation of security and privacy enforcing standards. The focus of EHR is to provide centralized repositories of data, however, aggregating and storing the data in a single place gives these vendor organizations immense power over the use of patient data. These system applications are bounded by compliances in order to gain a license for functioning and hence it can be argued that the vendors are legally bound against misuse of sensitive data. Even though promises are made by such organizations against data misuse, internal attacks are still a valid threat. Verizon's data breach report [44] states that healthcare is the only industry having more internal actors behind cyber-attacks than external with privilege misuse having been cited

as one of the top three causes. The earlier concepts of EMR or paper records never presented any considerable threat in the event of unintended disclosure. However, with an ever-increasing centralization of data, it has become extremely easy for malicious actors to obtain almost all personal data with a single breach. The medical data of a patient is very valuable, as it also holds a patient's personal information such as name, numbers, addresses, financial details, etc. apart from medical records. Hence, disclosure of this data in the wrong hands can result in identity theft as well as possible blackmail. The only way to tackle this is through the use of encrypted data both for storage as well as transmission, some of which were discussed in Section 5.3.

5.5.1.3 Problems with data sharing

A patient's medical records play a crucial role in the healthcare research industry. According to the ONC report [45], researchers in the field of the health industry need to analyze information from a variety of source. This is a must in order to mitigate risks, develop new cures, and enable the advancement of the medical industry in forming new treatments. The problem is that strict regulatory requirements and compliances make it harder for healthcare service providers to extract patient data for research purposes. Moreover, the ever-increasing incidents of data breaches and privacy problems do not help the case. In sections 5.5.2 through 5.5.5, we discuss how blockchain is a suitable alternative and provide an overview of its architecture.

5.5.2 Blockchain overview

A blockchain is a digital distributed ledger consisting of blocks linked together through hash values. Each block consists of cryptographically signed transactions. A block is added to the chain by consensus between all participating nodes, therefore, maintaining consistency. The cryptographic linking of blocks and the replication of state across all nodes makes the blockchain immutable. Conflicts for block additions are resolved depending on the chain architecture and consensus algorithm followed. We shall dive into each aspect of blockchains architecture, discussing the various benefits, implementations as well as shortcomings.

5.5.2.1 Advantages of using blockchain

1. **Decentralized management:** The use of a distributed digital ledger is the driving force behind a blockchain implementation. A blockchain maintains the same state of data for every participant on the network, that is every user has the same copy of data. The primary purpose of enforcing this rule is to eliminate centralization. Traditional databases have a central trusted authority to manage the changes to the state of data; however, blockchain eliminates the need of this central trusted authority and the participants themselves are responsible for the policing of the distributed digital ledger. This means mis-trusting parties can also engage in the exchange of data without the need for a mediator.

2. **Robustness/availability:** As the database is distributed amongst all the participants and consistency is maintained at all times, it is ensured that the downtime of a few nodes cannot undermine the whole network making it extremely robust. Also, multiple distributed copies provide greater availability to the participants.
3. **Immutable records:** A blockchain is immutable, as in every block of data that are added this distributed ledger cannot be modified. This is extremely important from the point of security as an accepted state is permanently recorded. The immutable records also act as an audit trail of transactions on the network providing accountability.
4. **Nonrepudiation:** The transactions done by users are signed cryptographically. Hence, as a direct consequence of immutability and distributed ledger, a participant cannot deny having done a transaction that has been recorded on the distributed ledger.
5. **Anonymity:** Blockchain supports anonymity. The users can interact with the network through the addresses generated through their keys, hence preserving their privacy. All the transactions are cryptographically signed ensuring security.

These combined features allow blockchains to address the issue of a centralized EHR. The concepts of national cloud-based EHR systems discussed in Section 5.4.3 can be applied to applications developed using blockchain. This can support the existence of a single implementation that is managed by all participants and addresses the issues of interoperability as well. There will be better accountability through immutable auditable records. Patient-centric records can be functional without a compromise in security and privacy. A unified view of the patient record is possible through a singular implementation. Consented data sharing for advancing healthcare research will be much easier and flexible. In order to develop an understanding on how blockchain can achieve these benefits, we will establish an overview of the basics of blockchains, the challenges that it faces and the proposed implementations with respect to EHR systems.

5.5.2.2 Implementation

A blockchain consists of cryptographically linked blocks. Bitcoin, which was the first implementation of the blockchain, was developed as an electronic cash scheme, hence the data of the blocks consists of transactions. The data of the blocks can be repurposed depending on the application required. Each block has a header that is linked to the previous block through a hash value. Figure 5.7 provides a representation of a typical blockchain. Hashes have three significant properties: (1) they are unique, meaning a completely different hash values is generated even for a small change in the data; (2) they are one way, that means it is not computationally feasible to find any input that maps to prespecified output; and (3) they are collision resistant, that means it is not computationally feasible to find two inputs that produce the same output. The blocks are ordered according to the time at which they were added and hence the chain only increases in length. This linking of

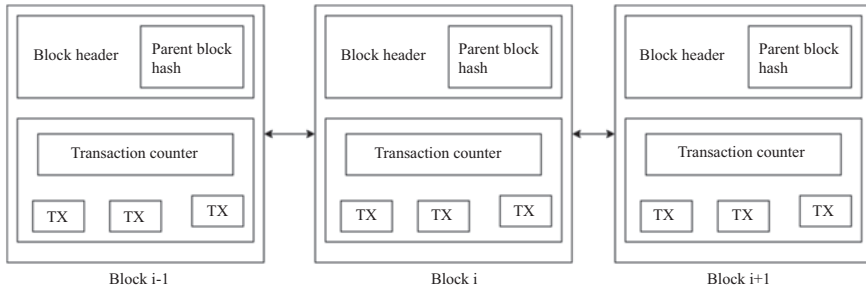


Figure 5.7 A representation of blockchain [46]

blocks through hashes provides the property of immutability to the blockchain as any change in the data of a block would have to be supported by a corresponding change in the block headers of all the blocks that were added after that block. Moreover, this change would have to be corroborated across the whole network in order to gain acceptance. The success of an attack on a blockchain through multi-user coordination depends on the consensus algorithm being used. Consensus algorithms are responsible for maintaining consistency amongst the nodes of a blockchain network and play a very important role in how the blockchain functions.

5.5.2.3 Public and permissioned blockchains

Blockchains can be broadly divided into two categories, that is, public and permissioned blockchains. Blockchains were originally developed with the intention to be public, with regards to eliminating any central trusted authority to police the network. Public blockchains place no restrictions on a user. Everyone can become a participating node, read the contents of the blockchain and contribute to the consensus process that advances the chain. Users of public blockchain interact through asymmetric key cryptography. A user is assigned an address on the network, which is usually the hash value of their public key. Any transaction that takes place on the network involves digitally signing the transaction using the private key.

This concept of blockchain, however, was not deemed useful by corporate organizations. In cases where a few organizations are collaborating together, they would neither wish their data would be made public nor for any unauthorized user to participate in the network. The concept of permissioned blockchain is similar in concept to that of public blockchains, except the fact that the access to the network is limited to a defined set of users. For example, for organizations which are a part of a supply chain network can deploy their own blockchain network. The nodes and users shall only belong to the participating organizations, and the rules for access and consensus shall be governed by the architecture of that blockchain.

5.5.2.4 Consensus algorithms

The consensus algorithm forms the core functionality of a blockchain network. It determines how new blocks are added to the network and how consistency is resolved amongst all the participating nodes. The first consensus algorithm is *Proof*

of Work. For a node to add a new block to the chain it first has to find a hash value that satisfies a certain property termed as hardness. This can only be solved through brute force and requires a lot of computation power. Nodes which engage in such tasks are termed as miners. Once a block is mined, it is broadcasted to all other nodes on the network which verify its authenticity and correctness. In case of multiple block proposals, forks take place and the natural rule is to select the longest chain amongst the forks. Proof of work is resistant to any malicious attacks such as distributed denial of service (DDoS) as proposing a new block requires a lot of computational work. However, a large number of expenses expended for computation require the miners to be compensated. Proof of work was proposed in bitcoin which would reward the miners with its own native currency for an accepted block. Most of the other implementations also revolve around digital cash, and hence their native currencies are used to incentivize the miners for their work.

Proof of Work was the only consensus algorithm for some time in the block-chain space; however, it has a number of disadvantages. The requirement of intensive computation has the following effects: (1) waste of a lot of energy, (2) miners become more limited and centralized as the difficulty rises, and (3) highly limited number of transactions can be performed for a given duration, resulting in extremely limited scalability. In light of these shortcomings, a number of alternative consensus algorithms have been proposed. *Proof of stake* involves random node selection based on account balance, with the theory being that accounts with more money are less likely to attack the network. *Delegated Proof of Stake* goes one step further by reducing the miners to a changing set of elected nodes further improving speed and scalability. The class of *Byzantine Fault Tolerant Algorithms* are the most secure and scalable, but most of them are suited for permissioned networks. The selection of a consensus algorithm hinges on the requirements from the network, such as whether it is public or permissioned, how are the nodes incentivized, what are the safety and security requirements, etc.

5.5.2.5 Smart contracts

The early versions of blockchain did not have any facility for automated codes. Public blockchains, such as Ethereum have tried to address this issue through the use of smart contracts. The Ethereum blockchain functions similar to a Turing state machine, with the blocks representing a particular state. The chain itself can store both data as well as code. These segments codes are known as smart contracts, they have their own addresses and can be triggered through transactions on the network. They can also employ access control mechanisms to ensure only authorized users can trigger the contracts. The data itself can be made encrypted to ensure privacy and protection.

5.5.2.6 Challenges

1. **Identification and confidentiality:** Blockchains support pseudo anonymity by referring to users through their addresses which are derived using their public keys. This, however, does not guarantee full privacy as the transactions can still be traced based on account activity associated with an identifier. Moreover, in medical applications, the participants need to be sure of the

identity of the party with which they are sharing their records. Thus, better ways of identification need to be established while also ensuring that the information is not disclosed to unintended participants on the network.

2. **Scalability:** The processing of transactions in the blockchain is time consuming. The consensus protocol plays a key role in determining the speed of transactions processing. Most of the earlier implementations used Proof of Work as their consensus protocol. The version of Proof of Work used by bitcoin is limited to a mere 3.3 transactions per second on an average which pale in comparison to centralized payments processing systems such as Visa, which processes about 2,000 transactions per second. Moreover, most of the earlier proposed consensus protocols did not scale well. In addition, the data processed by these transactions is extremely limited in its size. Hence, scalability overall is a particularly thorny issue. Two possible alternatives are (1) development of new consensus protocols and (2) data optimization. Permissioned blockchains have made significant headway in issues of scalability due to their partially centralized nature and process a much larger amount of transactions [47]. The other factor is the amount of data on the blockchain. Since blockchain is being considered as an alternative for various applications involving multiparty participation, the question is how to optimize the data. We shall be discussing a few of these methods that can both limit the data as well provide greater security and privacy.
3. **Possible attacks:** The data on the blockchain can be tampered by malicious parties. This depends on the percentage of the participants that are colluding to compromise the network and the consensus protocol employed. Proof of Work implementations requires majority nodes, that is, 51% of nodes need to collude in order to mount a successful attack. On the other hand, Byzantine consensus protocols, such as Tendermint and Practical Byzantine Fault Tolerance (PBFT) could be compromised at one-third faulty nodes. However, as these implementations are permissioned, the chances of this happening are pretty low. Such collusion attacks require coordination on a major scale and hence have a pretty low chance of success.
4. **Key management:** Participating in a blockchain network requires a set of public–private key pair. Unlike, centralized networks where a trusted authority maintains a server for key management, blockchains do not have a key storage facility. The users are responsible for maintaining their key sets. In the event of the loss of the private key associated with an account, there are no means to recover the associated contents or value associated with that account. The private key guarantees authenticity, decryption of data, and any transaction that a user wants to commit. Its loss means the definite closure of the account. Security wise, the theft of private keys is the most feasible and exploited attack on the blockchain network. Wallets provide a facility for users to manage their key sets, there are multiple implementations for these ranging from cloud-based options to hardware options. Management of keys and the absence of recovery options present the second most important challenge to practical applications of blockchain after scalability.

The use of blockchain in Healthcare Industry is in the early stages of exploration, and a few models have been proposed [48]. In the following section, we will discuss some solutions geared toward the application of blockchains in the healthcare industry.

5.5.3 *MedRec*

The MedRec distributed ledger system [49] provides a novel solution employing the Ethereum blockchain. It proposes the use of medical data aggregators as miners for a permission less decentralized personal healthcare records system. The system stores the data in encrypted form off chain using the work of Zyskind [4] which is discussed in Section 5.5.4. The permissions are on the chain and the ledger provides a record of transactions ensuring audits. Unlike other centralized system implementations, MedRec focuses on how anonymized sharing of data can be supported alongside other requirements of an EHR system.

The system consists of three types of actors. The users or the patients, the healthcare service providers, and the miners. The network supports three types of contracts, that is, registrar, summary, and patient provider relationship contract. Every entity on the Ethereum blockchain is recognized by their address. The registrar contract maps a given actors identification strings to their respective address. In the case of a user like a patient, this mapping would be singular, however, in case of the medical service providers, it will provide a mapping for all the patient relationships that it is managing. The target address, in turn, stores a summary contract.

The patient-provider relationship contract is between any two entities on the network, wherein one manages the data for the another. The contract contains query strings as well as the access and control permissions for specifying proper authorization and authentication. The query strings are affixed with hashed pointers to the medical data held off the chain by the service provider. The query strings can specify portions of the data. This allows for patients to specifically decide on what personal data do they wish to share. These query strings are then mapped to the address of the third party with which the patient wishes to share the data with. The queries that are allowed on a given set of data are decided by the service provider generating the data. The contract additionally also stores the service providers address, that is, hostname and port, so that the client knows where the database can be accessed in the network. The concept of using generic strings to query ensures convenience in dictating access control rules over data.

The summary contract which was the target address for the registrar contracts stores a reference to all patient-provider relationship contracts held by a user at any point in time. This contract acts as a nodal point for all the related data and relationships that belong to a user of the system. For example, a patient's summary contract would consist of references to all the service providers that the patient has been engaged with. On the other hand, providers will have references to the patients they are serving, as well as parties with which they are sharing their data. The MedRec system also supports notifications, which are triggered whenever a change

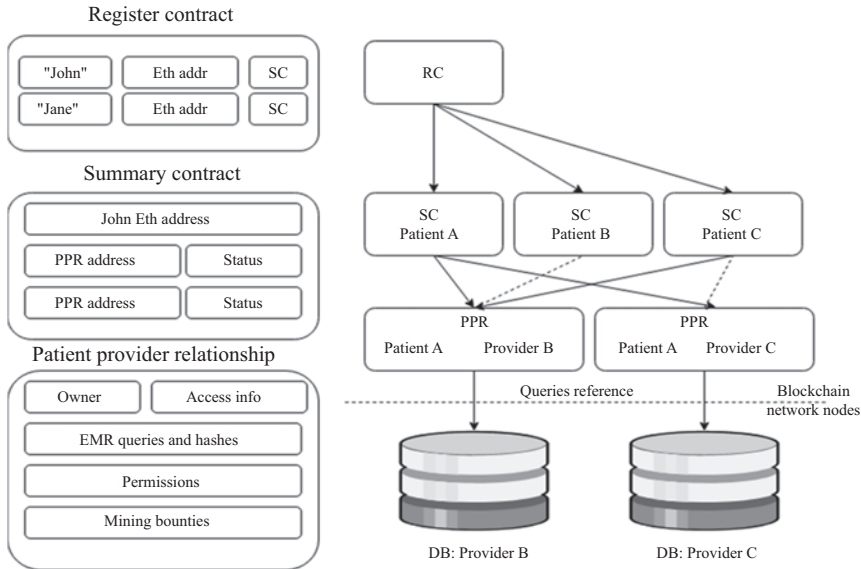


Figure 5.8 Smart contract employed by MedRec [49]

is made to a reference of a summary contract. In order to prevent spamming by malicious parties, these notifications are only triggered due to changes caused by a medical service provider. An overview of these relationships is provided in Figure 5.8.

5.5.4 Storing data off chain

Storing the data on the chain can prove to be cumbersome and computationally intensive. As stated before, the primary purpose of blockchains is to provide a verifiable transaction history visible and accessible to all participating actors. As each transaction has to be verified by a majority of nodes, data access, and retrieval procedures can be very slow as current implementations of blockchain are not scalable. To deal with this problem, solutions for storing off chain data storage have been proposed that can be both scalable as well as provide transaction history on the chain.

Zyskind *et al.* [50] developed an off chain personal data storage solution. The system supports two types of participants, users and services. A user can store personal data on the system. This data can include anything. While current applications work in a binary fashion which requires users to share information for using the services, the proposed solution provides fine-grained access control to the users. The services, however, can request user data in an anonymized fashion, hence preserving the identity of the users and providing the services with the data they need for their analysis.

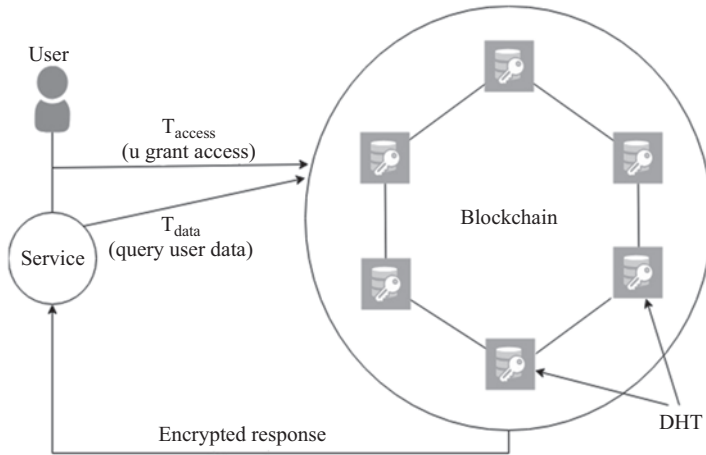


Figure 5.9 Representation of off chain data storage model [50]

An overview of the system is provided in Figure 5.9. The system supports two types of transactions, namely T_{access} , used for access control management and T_{data} , for data storage and retrieval. The data to be sent is first encrypted using symmetric encryption and then routed to an off blockchain key-value store. The ledger subsequently stores a pointer, that is, hash of the data. The end result is that the distributed ledger maintains a record of all associated access permissions including hash pointers to data stored off the chain. Any user or service that wishes to access the data would have to be first verified by the system through their digital signatures for whether they satisfy the access control rules. All the records concerning access, changes, and retrieval are maintained on the blockchain for audit purposes if required. The distributed hash table is an implementation of the one proposed by Kademilia *et al.* [51] using Level DB2 to provide added persistence and interface to the blockchain. As the stored data are encrypted, the nodes maintaining the network cannot read the data. In the scenario of nodes acting maliciously, replication provides fault tolerance and the attack can only succeed if the majority nodes work in coordination.

5.5.5 Identity and claims

In order for a blockchain-based EHR systems to be successful, it requires dealing with the challenges presented in Section 5.5.2.6. The development of self-sovereign identity systems presents solutions that are suitable for patient-centric EHR systems. Sovrin [52] is developing a decentralized self-sovereign identity network. The challenges faced by the identity industry are similar. The requirement of a single global implementation, a single viewpoint for identity related data, access control over what portions of your data are shared, revoking access to your personal

data, ensuring anonymity in identity relationships, and sharing of data anonymously. The implementations that have possible to tackle these issues shall be discussed in this section.

5.5.5.1 Decentralized identifiers

Sovrin employs decentralized identifiers (DID) for identifying users. A DID is a new type of identifier that is globally unique, resolvable with high availability, and cryptographically verifiable. DID infrastructure can be thought of as a global key-value database. The DID serves as a key and the value is a DID document. The purpose of the DID document is to describe the public keys, authentication protocols, and service endpoints necessary to bootstrap cryptographically verifiable interactions with the identified entity. The DID document is a valid JSON-LD object, and it includes the following components: (1) the DID itself, (2) set of cryptographic material, (3) set of cryptographic protocols, (4) set of service endpoints, (5) timestamps, and (6) optional JSON-LD signature. The DIDs can be created, read, updated, and deleted. The key purpose of the development of DIDs was to bake privacy into the design of identifiers. The DIDs provide flexibility in the fact that they can be used as well-known identifiers, or as privately issued identifiers on a per relationship basis.

5.5.5.2 Verifiable credential

A verifiable claim is a quality, achievement, qualification, or piece of information about an entity’s background. This can include government ID, payment provider, university degree, or name. The claim describes a quality or qualities, property, or properties of an entity which establishes its existence and uniqueness. Figure 5.10 provides a description of the structure of verifiable credentials and verifiable profiles. The verifiable ecosystem consists of (1) the Issuer, who issues verifiable credentials about a specific Subject, (2) the holder stores credentials on behalf of a Subject. Holders are typically also the Subject of a credential; (3) the Verifier requests a profile of the Subject. A profile contains a specific set of credentials.

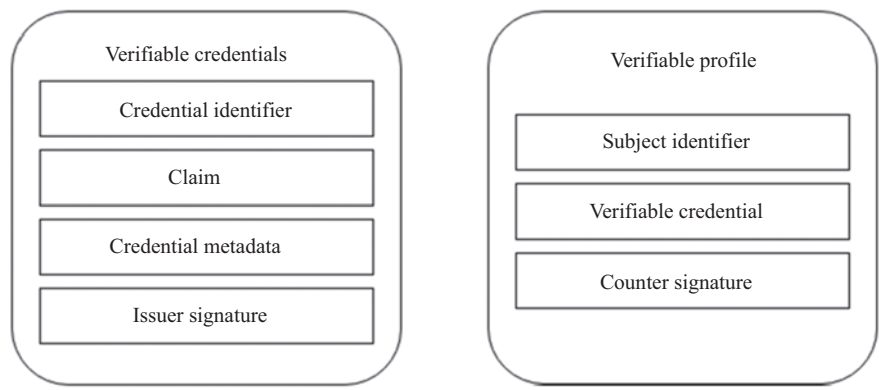


Figure 5.10 Structure of verifiable credentials and verifiable profile [53]

The verifier verifies that the credentials provided in the profile are fit-for-purpose; and (4) the Identifier Registry is a mechanism that is used to issue identifiers for Subjects. Another added benefit of these credentials is that they support the creation of schemas, which serve as machine readable definition of a set of attribute data types and formats. In other words, the schema definition serves as a template for claims. This means that direct programs can be written based on the schema to verify a claim.

5.5.5.3 Working of Sovrin

Sovrin maintains anonymity by declaring separate DIDs for every relationship. This ensures that no third party can establish any correlatability between transactions. As all the DIDs have cryptographic properties, the communication between the parties is verified through digital signatures. The application of DIDs shines through the use of claims. Claims can even be self-attested. If a user presents a claim, a third party can verify its authenticity through the digital credentials of the user. Similar to the DIDs, claims can be revoked or declared to be expired. Claims also have the property to be turned into disclosures, wherein a user might be interested in sharing only specific parts of the claim rather than the whole content. More importantly, the user can combine pieces of information from multiple claims to form a disclosure, and the verifier can still verify for the authenticity. This aspect is extremely powerful from the scenario of medical records. For example, a healthcare provider, after generating a new record can turn it into a claim for the patient. The patient that way will have access to all the records and can later allow for other practitioners to view those records (claims) depending on how much information they need. The patient also has the flexibility to revoke the claims. Claims are extremely flexible and can serve the purpose of proofs for later user. For example, a prescription by a practitioner can be turned into a claim for future use.

Sovrin employs a decentralized ledger using its own Plenum Consensus Protocol to store the DIDs. The plenum protocol is a version of the Redundant Byzantine Fault Tolerance Consensus Protocol (RBFT). The blockchain network used by Sovrin is permissioned. Sovrin has established a Trust consisting of major public and private organizations, maintaining diversity and equal representation. The use of a permissioned blockchain is twofold. First, only the valid nodes participate in the consensus protocol and do not have any incentives for mining, rather the governments and people will fund the functioning of the network just like any other subscription service. Secondly, the use of trusted nodes makes the task of the consensus protocol easier, hence the reason for selecting the BFT class of protocols. RBFT is resilient to attacks and supports fast recovery. The network has further divided the nodes into two broad classes: (1) validators and (2) observers. The validators support both read and write functionality, whereas the observers are simply used for reading the queried data from the chain. This division further improves the performance of the network. The reason for deploying a blockchain is to exploit the potential of DIDs and Verifiable Credentials as discussed previously. The DIDs and the claims presented above are similar to the public key infrastructure (PKI) for digital certificates, used for the purpose of verifying the

authenticity of websites. PKI has a number of certificate authorities that issue digital certificates. In order to verify DIDs and related claims, there needs to be a way to verify whether the cryptographic material belongs to the concerned party. Also, records need to be maintained for these to provide revocation facilities. One way would be to construct a facility similar to PKI, however, the centralization of the certification authorities would defeat the purpose of the system. The other way is to track the DID documents and claims through the blockchain.

Sovrin believes that personal data, including private DIDs, associated keys, claims, and other related stuff should be stored off the chain in a wallet like format. Figure 5.11 provides a description of the contents a wallet would store. The encrypted wallet can be stored on any cloud provider for better access and availability. Such providers have been termed as agents. Sovrin also states that only public DIDs, its associated documents, schemas, revocation registries, and agent authorization policies should be stored on the ledger. This ensures that issue claims can be verified by looking up the ledger for the required DID. This setup is extremely useful from the following perspectives: (1) storing the data of chain provides greater flexibility, makes the chain more scalable, and also ensures greater privacy and security even in the event of a compromise in network encryption;

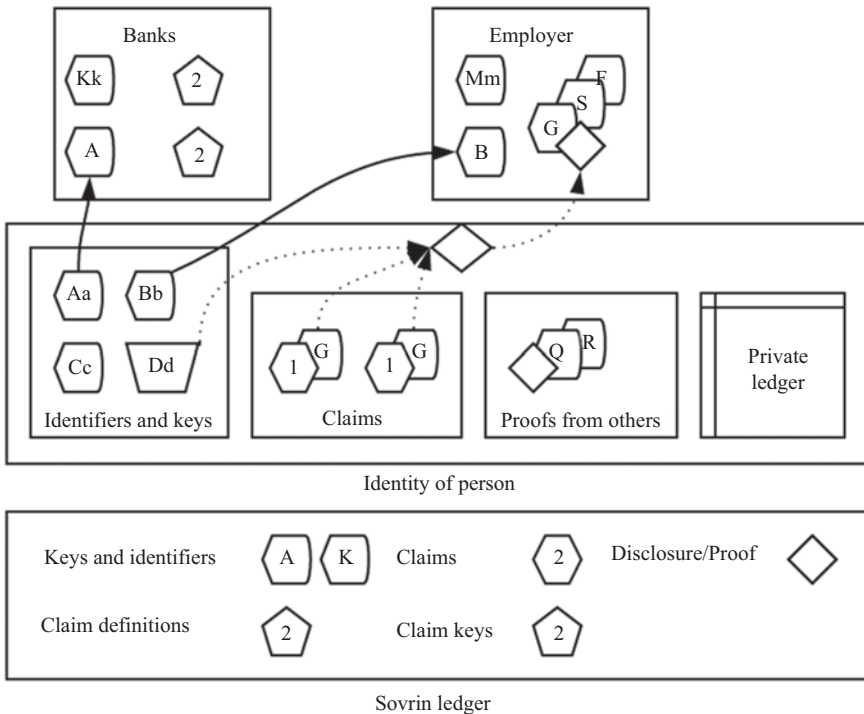


Figure 5.11 A representation of a wallet consisting of identity credentials in Sovrin [54]

(2) users have the freedom to move their data between any of the agents, as their data are not tied to any service. Lastly, both DIDs and verifiable credentials are unified standards maintained by the World Wide Web Consortium. This translates to the fact that they can be applied to any implementation of a decentralized ledger, hence ensuring interoperability.

5.5.5.4 Application for EHR systems

We finally round up the reasons on why the self-sovereign identity architecture is well suited for EHR systems:

1. Every patient can construct new DIDs for their relationships with different healthcare providers. Pairwise DIDs provide anonymity, hence no correlatability can be established giving maximum privacy.
2. Any form of medical data can be constructed in the form of a claim. These claims can have associated schemas defined according to the medical standards and hence predefined codes can automate the task of authentication and verification.
3. Every claim is cryptographically verified, hence ensuring the identities of participating parties are authentic.
4. Access control can work in the form of disclosures, as composite records can be created consisting of multiple claims.
5. Storing personal data in wallets increases data security and makes the chain scalable. A patient's data are like a personal data store. Hence the patient has total freedom to select which agent service to use for storing their data.
6. Audit logs are generated from the transactions on the chain regarding the exchange of claims. Hence ensuring accountability.
7. There is no central authority to trust. A consortium of healthcare providers and government organs can function as nodes for the ledger and charge the users basic fees for the same.
8. Data can be anonymously shared for research purposes. Moreover, as a block-chain is used, there is scope for the development of a native currency that can be awarded for data sharing. This currency can be used to foster the network, such as using it to pay the charges for network usage instead of real money.

DID and verifiable credentials are standards which means their future implementations in local EHR systems can be easily integrated with blockchain-based EHR systems.

5.6 Conclusion

The aim of this chapter was to shed light on the purpose of present EHR systems, identify associated shortcomings as well as necessary system requirements, and discuss methods and implementations that are being employed to solve these. A special emphasis was given toward how security and privacy can be preserved in these systems. Current implementations of EHR systems still have a long way to go

in order to achieve true unification of medical records. We established that the definition and requirements of EHR are vague, there is no definite structure and standards are multiple and nonuniform. This analysis was then used to present a few requirements that need to be fulfilled for the development of a successful EHR system. The subsequent section was focused on presenting various implementations that provide security and privacy in an EHR system. This was followed by a discussion on how these systems have matured in leaps and bounds, especially since the introduction of cloud computing. A few cloud-based EHR systems were discussed along with their implementations.

These cloud-based systems are liberating the previous implementations from the weight of hardware setup, maintenance issues, and problems of data fragmentation and hence expediting the timeline of production and delivery of EHR systems. However, they face a mounting challenge in the form of security and privacy aspects. Rising cybercrime incidents and the compounded risks associated with centralizing such sensitive information on a large scale presents serious issues to their validity for practical application. The introduction of blockchain presents an exciting opportunity for these EHR systems to truly achieve their objectives. To that end, we discussed advantages that blockchain brings to the table, presented an overview of how blockchain works and the challenges it faces. Finally, we presented some implementations that employ blockchain-based solutions and are suited for EHR systems. The future of EHR systems lies in patient-centric models. In systems that can be easily accessible to all actors in the ecosystem and yet are completely secure and privacy preserving. Research in this area shows a lot of promise and implementations such as Sovrin present new areas of applications that can redefine healthcare records.

References

- [1] Häyrynen K., Saranto K., and Nykänen P. "Definition, structure, content, use and impacts of electronic health records: a review of the research literature." *International Journal of Medical Informatics*. Volume 77, Issue 5, 2008, Pages 291–304.
- [2] International Organisation for Standardisation. (2014). Health Informatics – Electronic Health Record – Definition, Scope, and Context (ISO/DTR 20514).
- [3] Tange H.J., Hasman A., de Vries Robbé P.F., and Schouten H.C. "Medical narratives in electronic medical records." *International Journal of Medical Informatics*. Volume 46, Issue 1, 1997, Pages 7–29.
- [4] Ehnfors M., Florin J., and Ehrenberg A. "Applicability of the International Classification of Nursing Practice (ICNP®) in the Areas of Nutrition and Skin Care." *International Journal of Nursing Terminologies and Classifications*. Volume 14, Issue 1, 2003, Pages 5–18.
- [5] Kovner C., Schuchman L., and Mallard C. "The application of pen-based computer technology to home health care." *Computers in Nursing*. Volume 15, Issue 5, 1997, Pages 237–244.

- [6] MedlinePlus, Medical Dictionary 2005, available at: <http://www.nlm.nih.gov/medlineplus/plusdictionary> [Accessed April 3, 2006].
- [7] openEHR Community. openEHR. <http://www.openehr.org>. Creative Commons Attribution-NoDerivs 3.0 Unported.
- [8] Dolin R.H., Alschuler L., Boyer S., Beebe C., Behlen F.M., and Biron P.V. "HL7 clinical document architecture." Release 2.0. ANSI Standard, 2004.
- [9] HL7. HL7 reference information model. http://www.hl7.org/Library/data-model/RIM/modelpage_mem.htm
- [10] Vora J., Italiya P., Tanwar S., *et al.*, "Ensuring privacy and security in e-health records." *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, July 11–13, 2018, pp. 192–196.
- [11] Haas H.S., Wohlgemuth S., Echizen I., Sonehara N., and Müller G. "Aspects of privacy for electronic health records." *International Journal of Medical Informatics*. Volume 80, Issue 2, 2011, Pages e26–e31.
- [12] International Organisation for Standardisation. (2018). Health informatics – Electronic Health Record communication – Part 1: Reference model, (ISO/DTR 13606).
- [13] Westin A.F. "Privacy and freedom." *Washington and Lee Law Review*. Volume 25, Issue 1, 1968, Article 20.
- [14] Nate L. Top 10 Biggest Healthcare Breaches of All Time [online]. 2018. Available from <https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time> [Accessed January 26, 2019].
- [15] Fernández-Alemán J., Señor C.I., Oliver Á., Pedro L., and Ambrosio T. "Security and privacy in electronic health records: a systematic literature review." *Journal of Biomedical Informatics*. Volume 46, Issue 3, 2013, Pages 541–562.
- [16] Benaloh J., Chase M., Horvitz E., and Lauter K. "Patient controlled encryption: ensuring privacy in medical health records." ACM Workshop on Cloud Computing Security. Chicago, Illinois, USA, November 13, 2009, Pages 103–114.
- [17] Hu J., Chen H., and Hou T. "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations." *Computer Standards & Interfaces*. Volume 32, Issue 5–6, 2010, Pages 274–280.
- [18] Kanso A., and Ghebleh M. "An efficient and robust image encryption scheme for medical applications." *Communications in Nonlinear Science and Numerical Simulation*. Volume 24, Issues 1–3, 2015, Pages 98–116.
- [19] Tanwar S., Obaidat M.S., Tyagi S., and Kumar N., "Chapter 10: Online signature-based biometrics recognition." In M.S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature Switzerland AG 2019, pp. 255–285, 2019.
- [20] Tanwar S., Tyagi S., Kumar N., and Obaidat M.S., "Chapter 21: Online signature-based biometrics recognition." In M.S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature Switzerland AG 2019, pp. 535–568, 2019.

- [21] Science Applications International Corporation (SAIC). Role-Based Access Control (RBAC) Role Engineering Process, Version 3.0. 11 May 2004.
- [22] Mohan A., and Blough D.M. "An attribute-based authorization policy framework with dynamic conflict resolution." *9th Symposium on Identity and Trust on the Internet*, Gaithersburg, Maryland, USA, 13–15 April, 2010, Pages 37–50.
- [23] Hagner M. "Security infrastructure and national patent summary." IEEE Explore, *Tromso Telemedicine and eHealth Conference*, Guadelope, French Caribbean, 2–6 January, 2007.
- [24] Zhang R., and Liu L. "Security models and requirements for healthcare application clouds," *IEEE 3rd International Conference on Cloud Computing*, Miami, FL, 2010, Pages 268–275.
- [25] Harrington A., and Jensen C. "Cryptographic access control in a distributed file system." *8th ACM Symposium on Access Control Models and Technologies*, Como, Italy, 2–3 June, 2003, Pages 158–165.
- [26] Shamir A. "Identity-based cryptosystems and signature schemes." *CRYPTO 84, Advances in Cryptology*, Santa Barbara, California, USA, 1985, Pages 47–53.
- [27] Sahai A., and Waters B. "Fuzzy identity based encryption." *Advances in Cryptology – Eurocrypt*. Volume 3494, 2005, Pages 457–473.
- [28] Goyal V., Pandey O., Sahai A., and Waters B. "Attribute-based encryption for fine-grained access control of encrypted data." *ACM Conference on Computer and Communications Security*, Alexandria, VA, USA, October 30–November 3, 2006, Pages 89–98.
- [29] Beimel A. "Secure schemes for secret sharing and key distribution." PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
- [30] Crampton J., Martin K., and Wild P. "On key assignment for hierarchical access control." *IEEE Computer Security Foundations Workshop*, CSFW, Venice, Italy, 5–7 June, 2006, Pages 98–111.
- [31] Ateniese G., De Santis A., Ferrara A., and Masucci B. "Provably-secure timebound hierarchical key assignment schemes." *ACM Conference on Computer and Communications Security, CCS*, Alexandria, Virginia, USA, 30 October–3 November, 2006, Pages 288–297.
- [32] Narayan S., Gagné M., and Safavi-Naini R. "Privacy preserving ehr system using attribute-based infrastructure." *ACM Workshop on Cloud Computing Security Workshop, CCSW*, New York, NY, USA, 2010, Pages 47–52.
- [33] Chaum D., and Van Hejst E. "Group signatures." *EUROCRYPT*, 1991.
- [34] Rivest R., Shamir A., and Tauman Y. "How to leak a secret." *Advances in Cryptology. Asiacrypt*, Volume 2248, 2001, Pages 552–565.
- [35] Desmedt Y. "Threshold cryptography." *CRYPTO '89 Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*, Springer-Verlag Berlin, Heidelberg, 20–24 August, 1989, Pages 307–315.
- [36] Boneh D., Lynn B., and Shacham H. "Short Signatures from the Weil Pairing." *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, Springer, Heidelberg, Germany, 09–13 December, 2001, Pages 514–532.

- [37] Patra D., Ray S., Mukhopadhyay J., Majumdar B., and Majumdar A.K. "Achieving e-health care in a distributed EHR system." *11th International Conference on eHealth Networking Applications and Services*, Healthcom, Sydney, NSW, Australia, December 16–18, 2009.
- [38] Gul O., Al-Qutayri M. Chan Yeob Yeun and Quang Hieu Vu, "Framework of a national level electronic health record system." *BITS Pilani, Dubai International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, IEEE Xplore, Dubai, 2012, Pages 60–65.
- [39] Vora J., Tanwar S., Tyagi S., Kumar N., and Rodrigues J.P.C. FAAL: "fog computing-based patient monitoring system for ambient assisted living." *IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom-2017)*, Dalian University, Dalian, China, 12–15 October, 2017, pp. 1–6.
- [40] Hathaliya J., Tanwar S., Tyagi S., and Kumar N. Securing electronics healthcare records in Healthcare 4.0: "a biometric-based approach." *Computers & Electrical Engineering*, 76, pp. 398–410, 2019.
- [41] Kumari A., Tanwar S., Tyagi S., and Kumar N. "Fog computing for Healthcare 4.0 environment: opportunities and challenges." *Computers & Electrical Engineering*, Volume 72, 2018, Pages 1–13
- [42] Barua M., Liang X., Lu R., and Shen X. "ESPAC: enabling security and patient-centric access control for ehealth in cloud computing." *IJSN*. Volume 6, 2011, Pages 67–76.
- [43] Office of the National Coordinator for Health Information Technology. (2015). Report to Congress: "Report on Health Information Blocking." [Online] Available: https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf
- [44] Verizon. (2018). "Data Breaches Investigation Reports 2018."
- [45] Office of the National Coordinator for Health Information Technology. (2015). Report to Congress: "Report on Health Information Blocking." [Online] Available: https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf
- [46] Zheng Z., Xie S., Dai H., Chen X., and Wang H. "An overview of blockchain technology: architecture, consensus, and future trends." *IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 2017, Pages 557–564.
- [47] Vukolić M. "The quest for scalable blockchain fabric: proof-of-work vs. BFT replication." *iNetSec 2015: Open Problems in Network Security Lecture Notes in Computer Science*, Vol. 9591. Springer, Cham; 2015, Pages 112–125.
- [48] Vora J., Tanwar S., Verma J.P., *et al.* "BHEEM: a blockchain-based framework for securing electronic health records." *IEEE Global Communications Conference (IEEE GLOBECOM-2018)*, Abu Dhabi, UAE, December 09–13, 2018, pp. 1–6.
- [49] Azaria A., Ekblaw A., Vieira T., and Lippman A. "MedRec: using blockchain for medical data access and permission management." *2nd*

International Conference on Open and Big Data (OBD), IEEE Computer Society, Vienna, Austria, 22-24 August, 2016, Pages 25–30.

- [50] Zyskind G., and Nathan O. “Decentralizing privacy: using blockchain to protect personal data.” In *Security and Privacy Workshops (SPW)*, IEEE, 2015, Pages 180–184.
- [51] Petar Maymounkov D.M. “Kademlia: a peer-to-peer information system based on the xor metric.” In *Peer-to-Peer Systems, IPTPS*, Springer, Heidelberg, Berlin, Germany, 10 October, 2002, Pages 53–65.
- [52] Khovratovich D., and Law J. “Sovrin: digital identities in the blockchain era” [online]. Available from <https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf> [Accessed 26 Jan 2019].
- [53] Sporny M. “Verifiable credentials primer.” [online]. Available from <https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/topics-and-advance-readings/verifiable-credentials-primer.md> [Accessed January 26, 2019].
- [54] Philip J. Windley. “How Sovrin works” [online]. Available from <https://sovrin.org/wp-content/uploads/2018/03/How-Sovrin-Works.pdf> [Accessed January 26, 2019].

Chapter 6

Sustainable future IoT services with touch-enabled handheld devices

Davinder Rathee¹, Kiran Ahuja², and Anand Nayyar³

In today's hectic schedule numerous important tasks like servicing of our devices, switching off home appliances, purchasing essential eatables, and many other things which are important, usually skipped from our checklists. In order to resolve such issues many researchers/technicians have introduced the concept called Internet of things (IoTs). Home and industry, are two basic fields, where IoT has embed many new protocols or techniques to make things smarter. Everyone has a dream to make their home smart, where appliances communicate with each other and person himself monitors his home from anywhere. Today, it is possible to control refrigerator, treadmill, smart TV, light at home/office/industry from handheld devices. Latest gadgets are equipped with varied smart sensors like accelerometers, gyroscope, proximity sensor, GPS, barometer, magnetometer, ambient light sensor, Bluetooth, RFID along with long lasting batteries making them as smart handheld device. It may seem surprising today, but smart phones are going to manage IoTs movement in the near future. IoTs allude to expand interconnectedness of diverse smart gadgets over web. These gadgets include sensors and Internet which enable them to get, assemble, and transmit data by utilizing various connections, for example, Bluetooth, Wi-Fi, and so on. Therefore, the handheld devices can be considered as the user's ultimate device for IoTs interactions and control. In this era handheld devices are helping customers to order items online, application to check the items, or even enable user to track how big the queue is in the store, regarding the order of an item, and let customer when to pick it up. In addition to this, IoT devices also help the users to keep eye on fitness, track the steps, and so on. All emerging new technologies in smart handheld devices prove that MEMs can be the main candidate to achieve the IoTs movement in future. So, handheld devices are considered as a sixth sense for the current user and capabilities can be increased by integrating IoTs. In this chapter, the integration of handheld devices with IoT is described in detail and also gives a clear vision regarding the challenges and opportunities regarding the implementation in the real-world applications.

¹College of Engineering and Technology, DILLA University, Ethiopia

²DAV Institute of Engineering and Technology, Jalandhar, Punjab, India

³Graduate School, Duy Tan University, Da Nang, Viet Nam

6.1 Introduction

Internet of things (IoT) means connecting anything (device or service) at anyplace, anytime, and with any network. IoT is an emerging communication concept by which variety of devices, that is, from light bulbs to refrigerators, lawnmowers, washing machines and cars, meters, wireless sensors, and various networks connect efficiently and access the information remotely. All the devices connected and communicated seamlessly with similar endpoints like PCs, Laptops, tablets, and smart phones or something new future devices. Today it may seem fiction, but undoubtedly true that due to revolutionary invention of Internet with new kind of sensors and software/hardware is future either for human–human or human–device [1].

IoT promises a great future for new type of communication which is known as machine–machine (M2M) communication. We’re living in a world with smart sensors and smart devices which are all individually smart, make intelligent networks which can control from home appliances to industrial equipments, monitors themselves, send text information about location, pressure, and temperature, anywhere, anytime, on the planet. The number of connected devices increases up to 25 billion by 2020, while futuristic estimates are near to about 50 billion [2]. In addition to that as of December 2016, Google Play store was reported to host more than 2.6 million apps. To achieve such futuristic goals, hand handled devices must be smart, capable to access the Internet without Local Area Network (LAN) or Wi-Fi with independent its own power source. Such devices must be capable of collecting geolocations, temperature, health monitoring for human, animal, machines not for interaction with each other but also control as well. In this era of technology, we can order items online, also can select model, type, how much stock is left with the help of cloud and smart hand handled devices.

The Google trend graph Figure 6.1 showed a sharp increase in connected devices in 2015, another drastically increased in the year 2016, but in 2017 its inverses exponentially as shown by red line in Graph. It shows that interest in IoT technology seems on peak now a days, the expected number of connected IoT devices are more than 8 bn in use and around 7 bn non-IoT devices are connected in the network. So nowadays cars, machines, wearable devices, temperature controller, location detectors, and many other similar IoT devices are connected with many hand handled devices like PCs, tablets, laptops, and smartphone.

Today it’s really hard to imagine future without hand handled devises [4], these make connection off course automatically with IoT devices by using Wi-Fi. These make connection, collect information, do things automatically but till these don’t talk yet each other. Various applications like Alexa, Hue, Nest, and Sonos, individually these make our life better and provide the better degree of automation. Clients as of now use it for an enormous number of every day errands, for instance cooperating with keen gadgets. A large portion of the general population adjusts this change and feel like a natural movement. IoT isn’t simply going to be something we associate with in the home. IoT gadgets will be at school, in the workplace, in the nursery shed, and in our carports.

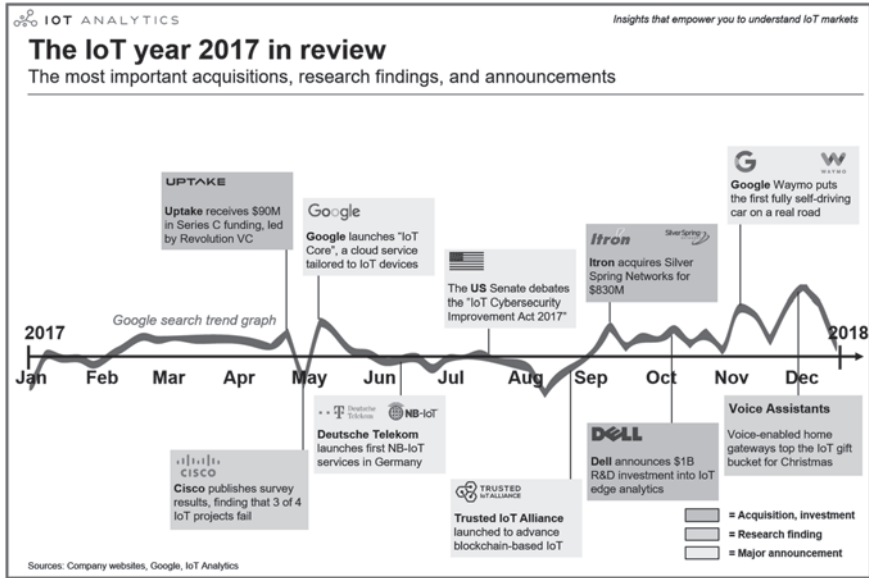


Figure 6.1 IoT review in year 2017 [3]

In this chapter, we give an overview about the hand handled smart devices integration with new emerging technologies for IoT, such as RFID, optical tags and quick response codes, etc. in Section 6.2. We discuss the architecture and real-world applications of IoT in the present era in Sections 6.3 and 6.4, respectively. In addition to that we describe the role of hand handled devices in the cloud environment using diverse offered services. Also, we put light on the networks used by IoTs as well as hand handled devices. The role of handheld devices in IoT system is described in Section 6.5. IoT networks versus handheld devices presented in Section 6.6. Finally, we discuss about expected challenges in the implementation and future of this amazing technology in Section 6.7. Conclusions are drawn in Section 6.8 and future scope is given for further research in this field.

6.2 Emerging IoT technologies

IoT components communicate with each other by two methodologies, that is, wired or wireless. Mainly 5 wireless technologies as shown in Figure 6.2 are the utmost important which can communicate seamlessly with standard protocols.

As the need of speed and security always in demand to accommodate the present requirement, so these wireless technologies are going to be prominent in future with conventional cellular networks, that is, GSM, LTE, and CDMA. The main IoT communication technologies are described as follow and their respective characteristics are tabulated in Table 6.1.



Figure 6.2 Top 5 wireless technologies for IoT [5]

Table 6.1 Characteristics-based comparison between top wireless technologies for IoT [5]

S. No	Technology	Standard IEEE	Frequency band (GHz)	Range (meters)	Applications
1		802.11	2.5–5	0–100	Mobile, smart devices, home/office networks
2		802.15.1	2.5	0–10	Mobile devices, medical equipments, smart devices and wearable
3		802.15.4	2.5	0–100	Sensor monitoring, industrial devices, IoT
4		802.15.4g	<1	0–20,000	IoT, smart cities, smart home, industries
5		ZAD12837 /ITU-T G.9959	<1	0–30	Home automation and sensor technology

6.2.1 Wi-Fi (wireless fidelity)

Now a days Wi-Fi technology gives freedom to connect the devices with local network and Internet without wire. It works on IEEE 802.11 standard which supports higher data rates with enhanced security. This mainly operates between two frequency bands, that is, 2.5 GHz and 5 GHz. It transmitted information with packet switching scheme, encrypt data for security purpose and follow TCP/IP protocol for transmission.

6.2.2 Bluetooth

Bluetooth technology was developed by Ericsson for short range communication suitable in hand handled personal devices. Bluetooth modules are simple to install into smart gadgets and these take flawless decision for remote headsets and wearable. It is likewise a standout amongst the best choices for remote sound streaming gadgets and smart human services frameworks.

6.2.3 Zigbee

Zigbee uses 2.4 GHz spectrum for communication. It works on low power mode and also best suitable for communication with diverse sensors. So, it may be best

suitable candidate for future IoT applications. It makes sure high security and efficiently transfers of data.

6.2.4 LoRaWAN

Low power wide area network (LoRaWAN) is a wireless communication technology; its most of the part is intended for IoT applications. All systems are associated by means of concentrated server unit. Various information rates can be executed by diverse frequency channels. It guarantees upgraded security at application and system level by utilizing a few layers of encryption. It is a suggested innovation for urban areas, smart home, and numerous other gadgets for modern mechanization and IoT.

6.2.5 Z-wave

Z-wave is a low power wireless communication technology particularly intended for home automation. It is best appropriate for computerized light controls and gathers information from sensors remotely. Z-wave utilizes ISM range beneath 1 GHz range. This is the least complex plan with less complicated protocol which work at low information rates.

The architecture of IoT systems for implementation of the above communication technologies in diverse applications is discussed below.

6.3 IoT architecture for diverse solutions

The International Telecommunications Union (ITU) has broadly classified IoT system into four different kind of structures, that is, tagging things, feeling things, shrinking things, and thinking things.

Tagging things: Connected objects traced and identified by using RFID tags, IR sensors, and PIR sensors.

Feeling things: As human body equipped with millions of sensors in the similar way IoT networks can be able to sense shrouding using modern sensors like temperature pressure, humidity/moisture, and LDRs.

Shrinking things: The tremendous growth in nanotechnology produces nano-sensors for measuring various parameters like water quality, gas leakage, and CO₂ conversion from environment gases similar to tree.

Thinking things: Smart networks are the future need for IoT where all users' human-human, machine-machine must be capable to communicate with advanced schemes seamlessly, maintain themselves automatically, and capable to transfer information and can make independent decision [6].

The most common architecture of IoT described by using layer system as shown in Figure 6.3. First layer named as object layer, it is equipped with different kinds of physical objects like IR sensors, PIR sensors, LDR, actuators, cameras, etc. for collecting of data from heterogeneous environment. The collected data are then transferred shown in Figure 6.3 via object abstraction layer by using latest communications technologies RFID, 5G, 4G, Wi-Fi, Bluetooth, ZigBee, Lora, Z-Wave,

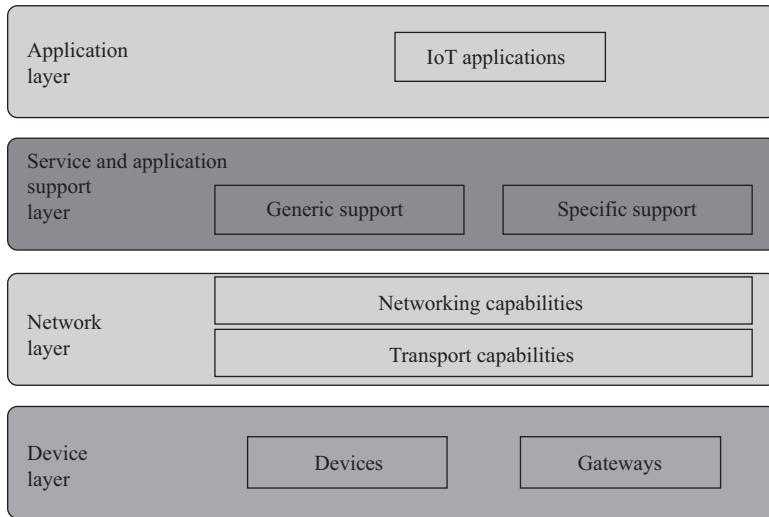


Figure 6.3 Layered architecture of IoT [6]

and also handles data cloud computing. Then the intermediate layers known as service layer process, these data provide services to the desired users in the networks. The fourth layer is known as application layer, it provides services to exclusive domains like smart parking, healthcare, and traffic management in order to meet their specific needs. The final layer named as business layer, it is used for analyses or huge data which supports in decision-making process and controls all the lower layers for their effective working, including maintaining their privacy [7].

The main sensors which extensively being used in IoT world are below:

Temperature/humidity sensors: This sensor used to gauge the measure of warmth from encompassing and convert the got information reasonable for different gadgets in system either by the rule of thermo coupling or resistor temperature detectors (RTD). Different sort of temperature sensors are appeared in Figure 6.4.

Thermocouples: Change its voltage regarding (w.r.t) change in temperature.

RTD: Change in resistance is legitimately relative to temperature change.

Thermistors: Changes its physical resistance w.r.t temperature. It is a temperature delicate resistor that changes its physical obstruction with the adjustment in temperature.

IC (Semiconductor): This great sensor gives temperature perusing legitimately on computerized shows and chips away at the guideline of conductivity changes with temperature varieties.

Humidity sensors: Humidity checking is one of the significant parameters for industry assembling process. It can be estimated as far as relative humidity (RH), dew/ice point (D/F PT), and parts per million (PPM).

Proximity sensors: This sensor is used to sense the presence or absence of object contactless, that is, in case of smart devices especially mobile phone

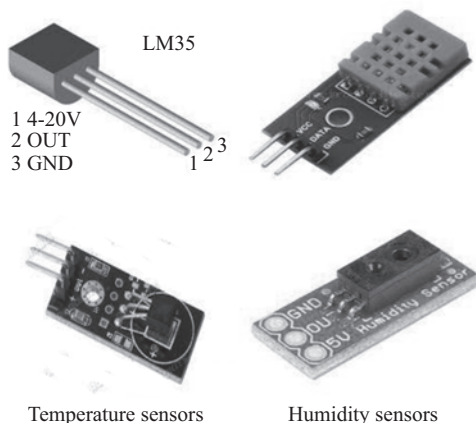


Figure 6.4 Temperature and humidity sensors

when you bring the mobile near your ear during call receiving it makes the screen brightness off in order to make battery life longer. Basically, it consists of pair of transmitters as LED which transmits Infra-Red light and receiver as photo detector which will receive the bounce back signal. Another good use of this sensor in cars, while taking reverse, they start to beep sound if any obstacle is there. But now with IoT these can be used to make smart parking in smart cities, airports, railways stations, or any public place. In addition to that these sensors can be programmed in online shopping to display huge discounts and immediate offer available for user. Different type of proximity sensors available in market as shown in Table 6.2, which are classified on behalf of working principle.

Pressure sensors: These convert the applied pressure into electrical signal and alert the user. Popular pressure sensor, that is, BMP180 shown in Figure 6.5 is used in mobiles, PDAs, navigation system GPS, smart vehicle, and aircrafts as well as tyre pressure monitoring system (TPMS).

With the IoT these sensors make possible not only to control manufacturing industry but also for the maintenance of water monitoring and heating system.

Smoke/gas sensors: Earlier smoke sensors were used for homes and industry safety purpose but now with the advent of IoT enhance the scope both sensors in field or safety and convenience. The commonly used smoke and gas sensors are shown in Figure 6.6. Due to integration with communication techniques, these sensors extend the wireless connectivity which may be deployed in various IoT applications. These sensors will detect the presence of smoke and flame in surrounding and generate alert alarm immediately in order to protect the life of people working in dangerous environments.

Gas sensors are used mainly in manufacturing pharmaceutical and petrochemical, agriculture for pesticides, air quality for detection of harmful gases, coal mines, paint, oil and gas industries, etc.

Table 6.2 Diverse proximity sensors [8]

Proximity sensor comparison			
Technology	Sensing range	Applications	Target materials
Inductive 	<4–40 mm	Any close-range detection of ferrous material	Iron Steel Aluminum Copper etc. 
Capacitive 	<3–60 mm	Close-range detection of non-ferrous material	Liquids Wood Granulates Plastic Glass etc. 
Photoelectric 	<1 mm–60 mm	Long-range small or large target detection	Silicon Plastic Paper Metal etc. 
Ultrasonic 	<30 mm–3 m	Long-range detection of targets with difficult surface properties. Color/reflectivity insensitive.	Cellophane Foam Glass Liquid Powder etc. 

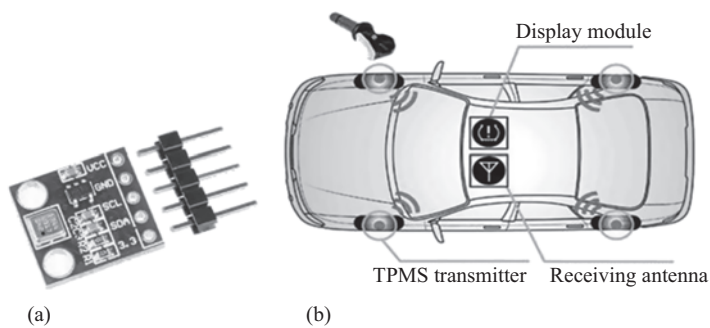


Figure 6.5 (a) BMP 180 and (b) overview of TPMS [9]

Motion sensors: This cost-effective passive infrared (PIR) sensor HC-SR501 shown in Figure 6.7 have lot of uses like toilet flusher, hand dryers, door controls as well as in automation of home and commercial and industrial security system.

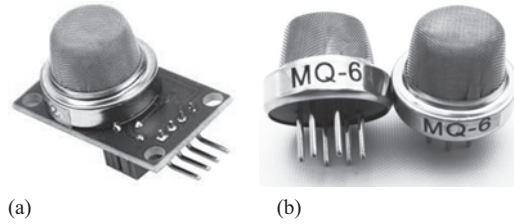


Figure 6.6 (a) Smoke sensor and (b) gas sensor



Figure 6.7 PIR motion sensor

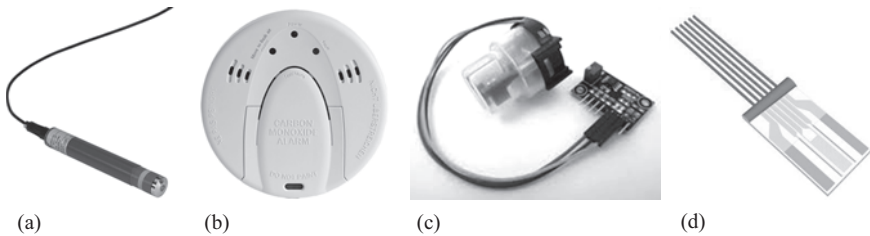


Figure 6.8 (a) Chlorine sensor, (b) carbon sensor, (c) turbidity sensor, and (d) conductivity sensor

Water quality sensor: To measure the water quality in terms of contaminants, that is, chlorine, carbon suspended solids for human use, and need to measure conductivity for industry purpose. So main sensors required are chlorine residual sensor, organic carbon sensor, turbidity sensor, and conductivity sensor as shown in Figure 6.8.

As water is the basic need it is clear that there is no life without water, so these sensors can play major role for measuring quality of water for different purposes. Additional pH sensors can be used to measure the acidic or basic nature of water.

Chemical sensors: These can be applied to monitor pollution in major cities. The basic aim is to check changes in air chemical and to detect the harmful gases. These can be used in industrial environment for chemical, explosive, and radioactive detection which is not be detected by human being before accident. Main sensors used are chemical field-effect transistor,

gas, chloride sensors, hydrogen sulfide sensor, and zinc oxide nanorod sensors as shown in Figure 6.9.

IoT gateways facilitate the interpretability of connected devices and also the bidirectional data transfer between networks and other components of networks by using some protocols. IoT cloud is basically high-performance network which optimized to process high speed data processing for all heterogeneous devices in network. IoT clouds collect, process, manage, and store big amount of data in real time and having capability to take action or decision as shown in Figure 6.10. Database management system (DBMS) is the most important candidate for IoT cloud.

Further, analytic process helps to convert analog data received from millions of sensors into useful coding, which help for editing, correcting, and transmitting for relevant action. Obviously, the interfaces are the visible and tangible part of IoT

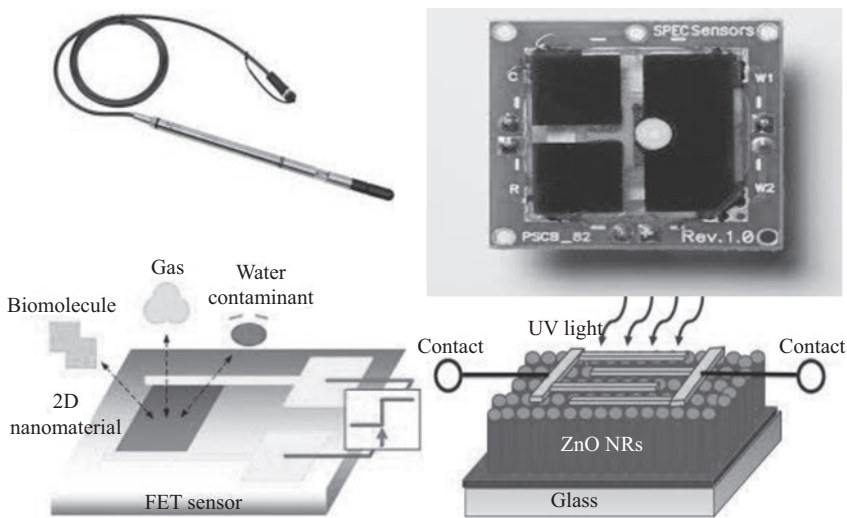


Figure 6.9 Chemical sensors

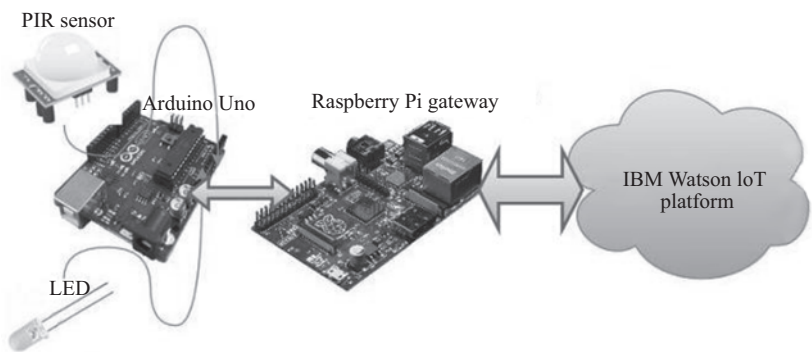


Figure 6.10 Bidirectional transfer of data for heterogeneous networks [10]

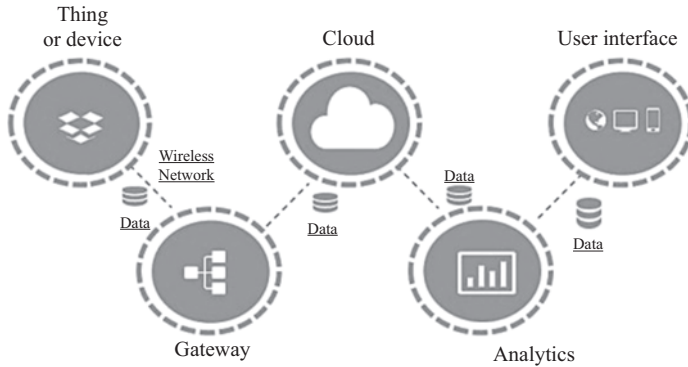


Figure 6.11 Main components of IoT [3]

system, which may be multicolor touch panels, hand handled devices, or some other smart gadgets. The only concern is these must be user friendly and compatible with common wireless standards. As the excel in technologies such as RFID and barcodes, actuators, sensors, and smart appliances give freedom to connect and communicate with each-other by IoT services through Internet [10,11]. The major components of IoT system are shown in Figure 6.11.

To design such automated and intelligent platform, different technologies are required to be clubbed to address these specific features of every application. The major real-time applications of IoTs in diverse fields are discussed in following section.

6.4 Real-world application areas of IoTs

In this era of modernization, the revolution in communication, IoT, and sensors made work easier, automated, and computerized. This resulted in more leisure as well as new health issues. Though it's the destiny to achieve the improved quality of life for the people enabling IoT to drive many possible applications in many domains such as healthcare, agriculture, smart parking, supply chain management (SCM), transportation or traffic handling, environment and disaster monitoring, etc. The major applications which have impact on the routine life of the users are described as follows.

6.4.1 Healthcare

IoT guarantees for alluring applications for health checking such as elder care, wellness of people, remote health observing, for example, BP, sugar, and so on, consistently, in addition to this it recommends treatment and prescription at client end. To develop such framework without doubt scientists in field of ICT, electronics and medical field need to work out more genuinely so as to make expansive vision of brilliant e-health framework. Along these lines, there is need of demonstrative and imaging gadgets, sensors having ability to interface with cloud for giving social insurance administrations at decreased expense to expand the personal

satisfaction [12]. Also, the primary consideration is on health observation for human, creatures and machines in keen urban areas by utilizing infrared thermography (IRT) [13]. The fundamental standard to gather the data is capturing of radiation emanating from body under scrutiny [14]. IRT has numerous applications in the field of prescription [15], support, and routine checking [16]. Electrical as well as mechanical support keeps away from exorbitant breakdowns [17]. Issue discovery is affirmed because of irregular examples of temperature estimation particularly in electrical types of gear [17]. Over the top division might be detectable if there should be an occurrence of mechanical devices. Especially concentration on rural health many solutions were already implemented for improving human health in rural area. RFID tags were distributed for users under investigation and registered for rural healthcare center (RHC) [18]. Main parameters which can monitor easily are temperature, blood pressure, etc. Tracking and monitoring using wearable can be used to capture health information and may communicate among the patients' homes, the hospital information centers, and other medical care system to make life secure [19,20].

6.4.2 Smart home/office/buildings

Smart homes and offices are the future in which air-conditions will be ON before you enter to home/office also light will be OFF automatically as you out from your place. The door will be unlocked for your friends for temporary while you are in your office. So, no surprise when IoT companies making life so simpler and convenient. Such facilities can bring revolution especially in residential colonies where everything will be under controlled by hand handled devices. Such smart homes and offices expected to promise save energy, time, and money. Smart home companies like Nest, Ecobee, and August are shaping future homes planning to deliver never seen before [20,21]. Example applications include monitoring of utility meters, energy, and water supply to avoid leaks or overloading, and gardening sensors, which could be used to water plants according to their needs and measure their vitals such as light, moisture, and humidity [22].

6.4.3 Wearable

Giant companies like Google and Samsung are investing heavily to build such devices like smart watches, wrist bands, chip implants, etc., which can take care of fitness, health, daily routine alert on critical condition, etc. Such devices will be loaded with sensors and software's which are capable to collect information and data about users.

6.4.4 Logistics and supply chain management (SCM)

Now a days in super markets track items in real time are using WSNs, barcodes, and RFIDs one by one, but in near future machines will decode full overloaded trolley in one time only with the help of IoT and varied transmission protocols such as 2G, 3G, 4G, and 5G. By the use of IoT and sensors opening scope for better control on the product quality from manufacturer to recycler as well as for location to mobility management [23–26]. Smart logistic entities are tracking items and protect these from thieves by using sensors which trigger alarms. When the

required conditions are met then unique addressability by employing various technologies such as RFID and WSNs to track the right product, at the right time, in right quantity at the right place having right price.

6.4.5 Transportation

IoT is providing better solution for road condition monitoring and alert systems [21,27] as well as for many other additional applications like license plate identification [28], finding parking spaces, and securing the vehicles [29] real time and alert in emergency like accidents [30]. Major brands like Tesla, BMW, Apple, and Google are working on bringing the next revolution in automobiles. It is expected that futuristic vehicles launch soon.

6.4.6 Alerts for disasters

The basic sensors of IoT are capable to collect and transmit environmental information such as temperature, humidity, and pressure. WSNs and mobile communication networks (such as 3G and 4G) are helping to communicate the sensed data to other users/systems and trigger the required alerts, and other participatory sensing data transmissions. Examples of such systems in literature [31] are available such as Health Monitoring and Risk Evaluation of Earthen Sites (HMRE2S) model.

6.4.7 Smart agriculture

Smart sensors monitor soil moisture, humidity, nutrition, and also help in proper fertilization and watering system. Smart farms share their data with other farmers, consumers, regulators, and with farm owners. RFIDs and 3D accelerometers are used to monitor animal tracking, livestock of disease and accidents, and also provide better prospects for husbandry [31].

6.5 The role of handheld devices in IoTs

The emerging life changing technologies make our hand handled devices smart enough for providing a ubiquitous and pervasive computing environment seamlessly and silently. These smart hand handled devices keep connectivity everywhere, and grant permission to access services anytime from any location through heterogeneous structures of IoT [11]. The emerging development in hardware,

Table 6.3 Roadmap for expected number of connected devices in IoT networks [11]

Year	Number of connected devices
1990	0.3 million
1999	90.0 million
2010	5.0 billion
2013	9.0 billion
2015	1.0 trillion

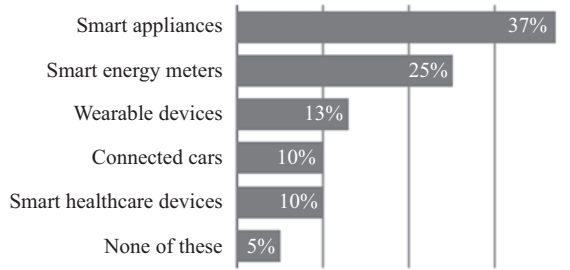


Figure 6.12 GSMA report [11]

sensors, and ICT techniques are attracting researchers to make ever bigger heterogeneous networks of sensors, communication technology, and Internet. There is no surprise, if the expected number of connected devices by next decade will be assumed more than 1 trillion as shown in Table 6.3.

A survey held by KRC research in UK, US, Japan, and Germany predicts that revolution in IoT industry going to attract the attention of users for smart appliances like smart phone as shown in below Figure 6.12.

CISCO declares that IoT will generate \$14.4 trillion business in next decade across all industries, which going to change the way of life drastically beyond imagination. Such huge networks must be controlled by hand handled devices or some other similar smart gadgets.

6.6 IoT networks versus handheld devices networks

The continuous higher demand for more battery life, less cost, and maximum wireless coverage resulted in new cellular networks. Major companies Vodafone, Cisco, Samsung, and Softbank are working on building national wide IoT networks [32]. They are working to meet the future requirements of cellular networks for successful implementation of IoT networks. Major issues for implementation of IoT networks are as follows:

6.6.1 Required long battery life

Archiving years of battery life is expected for IoT components after installation in order to reduce the overall cost. While in present communication scenario mobiles or any handheld devices lose most of their batteries due to hand-off mechanism. In this process device has to communicate multiple times per second with the tower. But in order to meet the requirement of coming IoT era it is expected that devices should spend most of their time in sleep mode [32].

6.6.2 Network scalability in heterogeneous environment

The IoT networks composed of millions of different kinds of sensors, which can be deployed in cells by uneven distribution. So, IoT networks must be capable to handle from a temperature measurement sensor to tracking services or more advanced services and diverse applications with higher throughput rate [33].

Table 6.4 Features of 5G technology [22,32,33]

Parameters	Femtocells	Pico cells	Microcells
Coverage range in meters	10–50	100–250	500–2500
Power in watts	0.100	0.250	2–5
Number of users	8–16	32–64	200 and more
Media	Wired, fiber	Wired, fiber	Wired, fiber connection, and microwave links
Applications	Indoor (primarily for indoor application, can be used for outdoor applications)	Indoor applications offices, hospitals, shopping centers, and schools	Outdoor applications

6.6.3 Required low deployment and adaptability cost

IoT components must have to accommodate themselves with in the cellular/handheld devices network as the cost for sensors deployed is very less than smart devices. So, there may be need of software up gradation, IoT networks must be designed to communicate in unlicensed bands or guard bands of cellular networks for the purpose of avoiding interference [22]. IoT networks must have coverage in basement, rural fields, in door areas, etc., which was not that much important in cellular networks, so IoT looking for new technology which can promise high data speed with reliable communication.

So, it is expected that 5G going to meet all IoT requirements because of its small cell concept. Further these small cells classified in three different groups, main features of these are shown in Table 6.4. It is clear from the table that 5G networks are the most favorable candidate for the future IoT connectivity. 5G seems to be solving all the limitations of traditional networks which is specially designed for high speed mobile broadband connection up to few gigabytes per second rate.

Femtocell networks are best for extended coverage specially required for deep coverage in underground building. While pico cells are good for extended network coverage and data throughput, so may be best for small enterprises use. If the number of users is more, then microcells architecture can be selected. So, it seems that all limitations of traditional network can be overcome by 5G.

There are numerous advantages of 5G technology, some of the main advantages have been described below:

- It has bidirectional large bandwidth shaping facility with high resolution provision.
- It has capability to gather number of technology networks on one platform.
- It is more effective and efficient as compared to existing technologies.
- It facilitates subscriber by supervision tools for quick actions.
- It provides broadcasting data range in Gigabits (Gbps), which supports more than 65,000 connections.

- It is scalable technology and easily manageable with the existing generations.
- It supports heterogeneous services as well as ubiquitous communication system.
- It provides uniform, consistent, and uninterrupted connectivity throughout the world.
- Multiple services parallelly possible with 5G technology. For example, user can check weather and location status while talking to another person at same instance.
- User can control remotely PCs by handsets or handheld devices.
- Education becomes easier by emerging 5G technology as a student sitting anywhere in the world can attend the class by video conferencing at high buffering speed.
- Medical treatment of the patients becomes easier and frugal as the doctor can check and treat the patient located in remote areas of the world.
- It makes monitoring process easier as governmental organizations investigate and can monitor anywhere, which directly resulted in reduction of the crime rates.
- It is possible to visualize the universe, planets, and galaxies by emergence of 5G technology.
- It becomes easy and very much possible to search and locate the missing persons/things/devices.
- It becomes possible to predict natural disaster such as earthquakes, tsunami, etc. which requires faster detection.

Some distinguished disadvantages of 5G technology are as following:

However, 5G technology is conceptualized and researched to solve the numerous problems in the field of radio signals and hardships in mobile world, but it has some security issues and lacks in technological advancement in most of the regions. Some major shortcomings are as following and pictorially shown in Figure 6.13.



Figure 6.13 Major shortcomings of 5G technology [34]

- It is still under process and presently also research is going on its viability.
- As the number of users are increased tremendously and connections are also increased in manifold so the speed claimed by this technology seems difficult to achieve as the incompetent technological supports in most regions of the world.
- All existing devices are not be competent to 5G technology, hence, there is need to replace them with new one, which is an expensive deal.
- The development of infrastructure for this requires high cost investment.
- Security and privacy are still such issues which need to be resolved yet.

6.7 Opportunities and challenges of IoTs with handheld devices

This is an era of smart devices and sensors, but yet these do not know how to communicate with each other, though data from smart watches/Fitbit can be accessed on your hand handled device or in your laptop but it's not automated. There is need to empower the connectivity platform in such a way, so that all these devices communicate with each other just by single sign as Apple did with its new TV platform.

Smart homes setup must have to follow Nest, Ring, Alexa, or Home Pods for connectivity to make life little better, but what will happen when they clash? This definitely will be annoying. In positive side smart fridge will let user know about food stock inside it, expiring date, etc., also smart light will be off automatically when user out from his/her bedroom, AC of living room will start work before user enter there [35,36]. This is expected from future IoT. When some guest coming to home, door ring will recognize and slow down music inside bedroom and let user know without disturbing other members of family. To achieve all these, there is great need of smart powerful hand handled devices, that is, mobile, laptop, watches, glasses, etc. The major challenges faced by handheld devices with IoTs are as follows [37–53]:

Security challenges: This is serious issue: hacking of bank account, camera, reservation system, other PC monitors, etc. now a days is very common, so great attention is required across the world. In future, e-health system with the help of IoT is planned but Internet already suffered from IoT security attacks. Concern will no longer be just hacking of above items targets may be health even life for devil kind of people. The implementation of IoT in smart life is possible only by adding new shifts in security system. The basic reason behind the state of insecurity is neck to neck competition in market and race between vendors to show next innovative gadget connectivity by compromising with security. The developer and programmer are unaware of such issues, easily can be exploited remotely by hackers. IoT must have to overcome from lacks like computational power, large storage, and secure operating system, which cannot be invaded by intruders.

Privacy challenges: Some of the data collected by IoT devices is very sensitive and must be protected like Facebook and Google, the know more about us what we know. So, discarding of person data and sharing must be safer than copyright.

Future IoT industry will be comprising with ANN, these systems will keep habits, daily routines, and hobbies, what will happen if all shared with wrong person. Some solution must be provided for privacy by IoT management.

Connectivity challenges: Connecting of millions of devices with one network obviously will be biggest challenge. Presently we rely on centralized servers and log in with password, but imagine when millions of different devices will be communicating with each other. Some huge servers/clouds and peer to peer connection will be needed to handle such huge amount of data and to authenticate the users.

Compatibility challenges: As IoT growing in many ways with different technologies and standards, that is, Zigbee, Z wave, WiFi, etc., there is competition between them to become dominant transport mechanism in future which results to requirement of new hardware and software for connection.

6.8 Conclusion and future scope

IoT becoming incredibly popular it will not be a surprise if we say it is future which promise to provide the useful system for regular consumer and businessman. IoT taking the world in to atomization, soon everything from office to industry, shop to hotels, from car to airplane, everything will be interacted with IoT. The latest technology like 5G is going to bring revolution in IoT market. The predictions say wireless technologies will be capable to support billions of sensors effectively. Here, we provide an overview about the need of hand handled smart devices integration with upcoming technologies, that is, the IoT. The architecture and real-world applications of IoT in the present era are discussed in detail. In addition to this the role of hand handled devices in the cloud environment is explained for diverse services. The major five networks utilized by IoTs for communication with hand handled devices are explained and their respective characteristics are provided for specific real-time applications. The major role of handheld devices in IoT system is described with specific examples. IoT networks versus handheld devices presented for their comparison in positive direction. Expected challenges are discussed which are facing during the implementation and in future.

In future data connectivity will be ubiquitous everything around us will be smart like roads, eye glasses, restaurants, buildings, elevators, graze doors, kitchen drawers, cars, etc. Though IoT is its own early stage of development but powerful technologies of wireless communication make the whole system more cost effective, accessible and energy efficient. Day by day growth in IoT technology leads to adopt smarter devices. In future may be each smart device individually will be capable enough to communicate with other devices in same network or other networks. If such thing happens there will be no need any kind of control devices in future.

References

- [1] Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., and Kwak, K.S., 2015. The internet of things for health care: a comprehensive survey. *IEEE Access*, 3, pp. 678–708.

- [2] Mukherjee, P. The smartphone and the internet of things [Internet]. 2015. Available from: <http://praxis.ac.in/the-smartphone-and-the-internet-of-things/> [Accessed October 17, 2018].
- [3] <https://iot-analytics.com/iot-2017-in-review/>
- [4] <https://fossbytes.com/whats-inside-smartphone-depth-look-parts-powering-everyday-gadget/>
- [5] <https://www.rfpage.com/top-wireless-technologies-iot-5g-networks/> Top 5 wireless technologies for IoT and 5G networks [Accessed October 22, 2018].
- [6] Vongsingthong, S., and Smachat, S., 2014. Internet of things: a review of applications & technologies. *Suranaree Journal of Science and Technology*, 21(4), pp. 359–374.
- [7] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M., 2015. Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), pp. 2347–2376.
- [8] Nayyar, A., Puri, V., Nguyen, N.G., and Le, D.N. “Smart surveillance robot for real-time monitoring and control system in environment and industrial applications.” In *Information Systems Design and Intelligent Applications*, Springer, Singapore, 2018, pp. 229–243.
- [9] Tanwar, S., Obaidat, M.S., Tyagi, S., and Kumar, N. “Chapter 10: Online signature-based biometrics recognition.” In M. S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*. Springer Nature, Switzerland AG, 2019, pp. 255–285.
- [10] Nayyar, A., Puri, V., and Nguyen, N.G. “BioSenHealth 1.0: a novel Internet of medical things (IoMT)-based patient health monitoring system.” *International Conference on Innovative Computing and Communications*, pp. 155–164. Springer, Singapore, 2019.
- [11] Kumari, A., Tanwar, S., Tyagi, S., and Kumar, N. “Fog computing for Healthcare 4.0 environment: opportunities and challenges.” *Computers & Electrical Engineering*, 72, 2018, Pages 1–13.
- [12] Rathee, D.S., Ahuja, K., and Hailu, T., “Role of electronics devices for E-health in smart cities.” In K. Ahuja, & Khosla, A. (Eds.), *Driving the Development, Management, and Sustainability of Cognitive Cities, Practice, Progress, and Proficiency in Sustainability (PPPS)* (pp. 212–233). IGI Global Publishers.
- [13] Vora, J., Tanwar, S., Verma, J.P., *et al.* “BHEEM: a blockchain-based framework for securing electronic health records.” *IEEE Global Communications Conference (IEEE GLOBECOM-2018)*, Abu Dhabi, UAE, December 09–13, 2018, pp. 1–6.
- [14] Nayyar, A., and Singh, R. “Ant colony optimization (ACO) based routing protocols for wireless sensor networks (WSN): a survey.” *International Journal of Advanced Computer Science and Applications*, 8 (2017): 148–155.
- [15] Rani, P., and Ahuja, K., “Packet Switch Traffic Analysis in 3G (W-CDMA) System,” *International Journal of Advanced Engineering Technology*, Vol. 2, No. 1, pp. 141–146, June 2011.
- [16] Noethen, M., Wolter, K.J., and Meyendorf, N. 2010. Surface crack detection in ferritic and austenitic steel components using inductive heated

- thermography. *33rd IEEE. International Spring Seminar on Electronics Technology (ISSE)*, Warsaw, Poland, 2010. pp. 249–254.
- [17] Romero, J. Smartphones: the pocketable PC: is your phone smarter than a fifth grader? [Internet]. 2010. Available from: <http://spectrum.ieee.org/telecom/wireless/smartphonethe-pocketable-pc> [Accessed November 7, 2018].
- [18] Vasanth, K., and Sbert, J. Creating solutions for health through technology innovation. Texas Instruments. [Online]. Available: <http://www.ti.com/lit/wp/sszy006/sszy006.pdf> [Accessed December 7, 2014].
- [19] Information Society Technologies Advisory Group (ISTAG). Orientations for EU ICT R&D & innovation beyond 2013. 2011. Available online http://cordis.europa.eu/fp7/ict/istag/documents/stag_key_recommendations_beyond_2013_full.pdf [Accessed on June 12, 2018].
- [20] Asensio, Á., Marco, Á., Blasco, R., and Casas, R., 2014. Protocol and architecture to bring things into internet of things. *International Journal of Distributed Sensor Networks*, 10(4), p. 158252.
- [21] Lahiri, B.B., Bagavathiappan, S., Jayakumar, T., and Philip, J., 2012. Medical applications of infrared thermography: a review. *Infrared Physics & Technology*, 55(4), pp. 221–235.
- [22] Vora, J., Italiya, P., Tanwar, S., *et al.* “Ensuring Privacy and Security in E-Health Records.” *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, 11–13 July 2018, pp. 192–196.
- [23] Meola, C. *Infrared Thermography: Recent Advances and Future Trends*. Bentham Science: New York, NY, 2012.
- [24] Meola, C., and Carlomagno, G.M. Recent advances in the use of infrared thermography. *Measurement Science and Technology*. 2004, 15, R27.
- [25] Lasobras, J., Alonso, R., Carretero, C., Carretero, E., and Imaz, E., 2014. Infrared sensor-based temperature control for domestic induction cooktops. *Sensors*, 14(3), pp. 5278–5295.
- [26] Gorostiza, E.M., Lázaro Galilea, J.L., Meca Meca, F.J., Salido Monzú, D., Espinosa Zapata, F., and Pallarés Puerto, L., 2011. Infrared sensor system for mobile-robot positioning in intelligent spaces. *Sensors*, 11(5), pp. 5416–5438.
- [27] Purohit, R.C., Turner, T.A., and Pascoe, D.D., 2006. Use of infrared imaging in veterinary medicine. In J.D. Bronzino (Ed.), *Medical Devices and Systems* (pp. 725–732). Boca Raton: CRC Press.
- [28] Rohokale, V.M., Prasad, N.R., and Prasad, R., 2011. A cooperative Internet of things (IoT) for rural healthcare monitoring and control. In *2011 2nd IEEE International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)* (pp. 1–6). Chennai, India: IEEE Explore.
- [29] Vora, J., Devmurari, P., Tanwar, S., Tyagi, S., Kumar, N., and Obaidat, M.S. “Blind Signatures Based Secured E-Healthcare System.” *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, July 11–13, 2018, pp. 177–181.

- [30] Hathaliya, J., Tanwar, S., Tyagi, S., and Kumar, N. "Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach." *Computers & Electrical Engineering*, 76, pp. 398–410, 2019.
- [31] Vora, J., Tanwar, S., Tyagi, S., Kumar, N., and Rodrigues, J.P.C. "FAAL: fog computing-based patient monitoring system for ambient assisted living." *IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom-2017)*, Dalian University, Dalian, China, October 12–15, 2017, pp. 1–6.
- [32] Rathee, D., Sharma, R., and Rathee, R. 3-G technology in mobiles: a review. *National Conference on IT Research and Applications*, MAITM, Jagdhari, November 16–18, 2007.
- [33] Rathee, D., Kumar, M., and Arya, S.K., "Evaluation of TiO₂/SiO₂ dielectric thin films to overcome the challenges of CMOS scaling." *2011 IEEE Regional Symposium on Micro and Nano Electronics (IEEE-RSM2011)*, September 28–30, 2011, Le Meridien, Kota Kinabalu, Malaysia, IEEE Catalog No: CFP1168N-ART, ISBN-978-1-61284-846-4. doi: 10.1109/RSM.2011.6088273.
- [34] Li, R., Luo, H., and Bao, Z. Based on the Internet of things the supermarket chain management information system development and safety stock research. In *2010 2nd IEEE International Conference on Education Technology and Computer (ICETC)*, Vol. 2, pp. V2–368, 2010.
- [35] Tanwar, S., Thakkar, K., Thakor, R., and Singh, P.K. "M-Tesla-based security assessment in wireless sensor network." *International Conference on Computational Intelligence and Data Science (ICCIDS 2018)*, NorthCap University, Gurugram, April 07–08, 2018.
- [36] Nayyar, A., and Sharma, S. "A survey on coverage and connectivity issues surrounding wireless sensor network." *IJRCCCT*, 3, no. 1 (2014): 111–118.
- [37] Wei, Y. Design and realization of mobile information collection module in logistic Internet of Things unified information system. In: *Proceedings of IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, Xian, China, May 27–29, 2011. pp. 263–266.
- [38] El-Baz, D., Bourgeois, J., Saadi, T., and Bassi, A. ALMA, a logistic mobile application based on Internet of things. In: *Proceedings of the IEEE International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, August 20–23, 2013. pp. 355–358.
- [39] Soldatos, J., Kefalakis, N., Leontiadis, N., et al . D-3.4b: core aspire middleware infrastructure. 2010. Technical Report, Aspire FP7 Contract: ICT-215417-CP, 89 p
- [40] Government Office for Science. The Internet of things: making the most of the second digital revolution [Internet]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf [Accessed March 7, 2018].
- [41] Ghose, A., Biswas, P., Bhaumik, C., Sharma, M., Pal, A., and Jha, A. Road condition monitoring and alert application: using in-vehicle smartphone as internet-connected sensor. In: *Proceedings of the IEEE 10th International*

- Conference on Pervasive Computing and Communications (PERCOM Workshops)*; Lugano, Switzerland, March 19–23, 2012. pp. 489–491.
- [42] Ren, X., Jiang, H., Wu, Y., Yang, X., and Liu, K. The Internet of things in the license plate recognition technology application and design. In: *Proceedings of the Second International Conference on Business Computing and Global Informatization (BCGIN)*; Shanghai, China, October 12–14, 2012. pp. 969–972.
- [43] Haiying, W., Long, H., Xin, Q., Hongbo, W., Gechen, L., and Xianqing, D. Simulation system of the performance of power battery for electrical vehicle based on Internet of things. In: *Proceedings of the 2012 International Conference on Measurement, Information and Control (MIC)*; Harbin, China, May 18–20, 2012. pp. 681–684.
- [44] Shengguang, L., Lin, T., Yuanshuo, Z., and Rucai, Z. Internet of things for special materials transportation vehicles. In: *Proceedings of the IEEE International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*; Beijing, China, August 20–23, 2013. pp. 1891–1894.
- [45] Kyriazis, D., Varvarigou, T., Rossi, A., White, D., and Cooper, J. Sustainable smart city IoT applications: heat and electricity management & eco-conscious cruise control for public transportation. In: *Proceedings of the 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*; Madrid, Spain, June 4–7, 2013. pp. 1–5.
- [46] Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., and Kamal, T. A review on Internet of things (IoT). *International Journal of Computer Applications*. 2015;113(1). DOI: 10.5120/19787-1571.
- [47] Conrad, D. Three reasons carriers are building new cell networks for the Internet of things [Internet]. 2016. Available from: <https://techcrunch.com/2016/10/28/threereasons-carriers-are-building-new-cell-networks-for-the-internet-of-things/> [Accessed March 7, 2018].
- [48] Nokia. LTE evolution for IoT connectivity [Internet]. 2017. Available from: <http://resources.alcatel-lucent.com/asset/200178> [Accessed March 7, 2018].
- [49] Ericsson. Cellular networks for massive IoT [Internet]. 2016. Available from: https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf [Accessed March 7, 2018].
- [50] <https://www.machinedesign.com/sensors/proximity-sensors-compared-inductive-capacitive-photoelectric-and-ultrasonic>
- [51] www.mwrf.com
- [52] https://www.tutorialspoint.com/5g/5g_advantages_disadvantages.htm
- [53] Tanwar, S., Tyagi, S., Kumar, N., and Obaidat, M.S. “Chapter 21: Ethical, legal, and social implications of biometrics technologies.” In M. S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*. Springer Nature, Switzerland AG, 2019, pp. 535–568.

Part II

**Healthcare models, solutions,
and security standards**

This page intentionally left blank

Chapter 7

Existing enabling technologies and solutions to maintain privacy and security in healthcare records

C. Eben Exceline¹ and Jasmine Norman¹

Electronic health record (EHR) is a repository of a patient medical record stored in digital format. EHR is accessible by different healthcare professionals, administrative staffs, patients, and their relatives. The key highlight of EHR is that it is possible to exchange health information of patients between different healthcare providers. This EHR property supports patients with efficient and high-quality healthcare delivery. EHR has several advantages in improving efficiency, lowering costs, and medical errors. Usually, EHR is outsourced to the third party such as cloud or fog. These third-party service providers facilitate unlimited resources for storage and computing. This information technology infrastructure enables the medical record of a person to be stored in one place is accessed from any part of the world. Despite EHR's numerous advantages, it poses many security issues because EHR is exposed to third-party service providers and users of different kinds. Infringement of data privacy, data integrity, and user privacy are the main security issues. Researchers have come up with many ideas since 1982 to improve EHR's security. Then they concluded that these breaches of security might be confined by encrypting EHR before being outsourced to the third party. Researchers have used different encryption techniques to encrypt EHR, such as symmetric key encryption, public key encryption, and identity-based encryption. All of the above techniques of encryption fall with their common disadvantages. Currently, researchers apply attribute-based encryption (ABE) in EHR because it provides additional security requirement of flexibility and control unauthorized access. The ABE scheme allows the EHR owner to choose authorized users to access various parts of the EHR, and the EHR owner can enforce write access control and read user access control policies. Multiauthority ABE is developed to provide efficient key management and to avoid key escrow. Authentication of users can also maintain EHR's privacy and security. We discuss existing encryption techniques and authentication techniques in this chapter to maintain the privacy and security of EHR being outsourced to the third party. In addition, the advantage of enabling blockchain technology is also discussed in securing EHR.

¹School of Information Technology and Engineering (SITE), Vellore Institute of Technology, Vellore, India

7.1 Introduction

The vast development of digital technology replaced paper-based health records to electronic health records (EHR). Moreover, there are various shortcomings in paper-based health records (PBHR) [1]. First, it is inefficient because it is hard to analyze, resulting in poor healthcare delivery. Second, it is expensive in storing and transmitting from one place to another. Switching from PBHR to EHR helps patients to get healthcare services globally. EHR is maintaining patients' healthcare records in digital format. EHR contains patients' personal information, symptoms, medical history, demographics, lab reports, radiology reports, reviews, appointments, and medications. These data are susceptible, so EHR should be secured from malicious users. Global information says that EHR is more vulnerable to cyber-attacks when compared to bank details of a person [2]. It is necessary all over the world to protect the EHR of a patient.

At first, a client-server-based EHR is followed by all medical organization. They store and maintain EHR in local servers [3]. The limitations in client-server-based EHR is that the patient is responsible for the availability of his medical record in case of disaster. He should backup all the records regularly in multiple locations. Client-server-based EHR is less scalable. The medical organization needs to fix the server space and bandwidth before implementation. It is hard for updating, and it is more static. Speaking about the security of data in client-server-based EHR data theft happens or the data may be destroyed intentionally by hackers. Moreover, there is also a chance for malware to infect the system where EHR is stored. Moreover, other drawbacks in client-server-based EHR are implementation cost is high, and upgrading to new software or computer equipment is difficult.

Development in information and communication technology helped patients to store and share their EHR with others globally. EHR stored in one place is accessible from anywhere in this world and in any time using the most potent paradigm cloud computing. Cloud computing influenced Information technology industries, researchers, and cloud users because it provides many benefits. It lowers the expenditures, provides unlimited storage, increases computing efficiency, scalability, flexibility [4], and on-demand marketing. These benefits influenced the medical organization to store patient EHR in the cloud, so that patient can receive healthcare service globally.

Despite the fact that there are numerous advantages in receiving cloud computing, there are many security concerns in putting away patient's sensitive information in a third-party service provider. Data confidentiality, privacy, and user privacy are the prominent security concern in cloud computing [5]. Researchers used various encryption techniques and access control mechanisms to store and access EHR in cloud computing. They encrypted EHR before it is outsourced to the cloud. At first, the researchers used symmetric key encryption to encrypt EHR. In symmetric key encryption, each user has to maintain many keys. After that, they embraced public key encryption to defeat the inadequacies of symmetric key encryption. At this point, they advanced public key encryption with identity-based encryption by having the client's identity as a public key.

Then researchers discovered that attribute-based encryption (ABE) is appropriate to ensure security over EHR distributed to the cloud. As ABE ensures fine-grained access control and flexibility over EHR distributed to the cloud [6]. In ABE client is recognized by many attributes. ABE enables the data owner to enforce access control policies over his EHR. ABE is categorized as Key policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE access control policy is installed in clients key. The access control policy of client key ought to match the attributes related to the ciphertext [7]. In CP-ABE access control policy is installed along with ciphertext, and client key is installed with attributes [8]. The attributes installed in client key ought to fulfill the access control policy installed in the ciphertext to decrypt the message. By adopting CP-ABE to encrypt EHR, the EHR owner can depict access control policy expressively. However, a single authority ABE scheme suffers from user privacy.

Multiauthority ABE can be deployed to encrypt EHR to maintain user privacy. A distinct set of attributes are kept up by every authority. Multiauthority ABE can be deployed with a central authority and without a central authority. To provide a data owner-centric approach for data privacy, the data owner ought to be a central authority in issuing key to other attribute authorities. Researchers developed many multiauthority ABE schemes to secure EHR outsourced to the cloud [9]. One of the contributions is hierarchical ABE, where it provides a hierarchical structure to system users. Hierarchical ABE is advanced to attribute set based encryption where a single attribute holds multiple values. Key structure is given to matching the access control policy installed with the ciphertext. So the client can form attributes from different set to match the access control policy installed with the ciphertext.

Although the paradigm of cloud computing influenced Information technology industry and academic research, it does not satisfy many real-world needs [10]. In the application of storing and accessing patient EHR, each medical organization has its own cloud. For each encounter, the patient has to go to the same medical organization to update his EHR. In the real world, scenario patient may go to different medical organization for a health check-up. So medical records of a patient is scattered in different organizations. In case of emergency, a medical professional has to check all the previous medical history of a patient. This real-world need is not satisfied by the paradigm of cloud computing. The real world needs to access distributed data and is achieved by blockchain technology [11]. In blockchain technology, patient EHR can be scattered in distributed databases. The patient can permit anyone to access his EHR. Blockchain technology does not force anyone in the system to trust the third party. Thus it maintains user privacy and data confidentiality.

7.1.1 Contributions

The contribution of this chapter is:

1. The existing technology to maintain the privacy and security of EHR outsourced to the cloud is elucidated.
2. The shortcomings in the existing technology are elaborated.

3. Recent developments in maintaining privacy and security of EHR are explained.
4. Comparison between various technologies in maintaining privacy and security of EHR is provided.

7.1.2 *Organizations*

This chapter is organized as follows. Section 7.2 explains the existing technology to maintain the privacy and security of patient health information. In Section 7.3, we present the security requirement needed to store and access patient health information. In Section 7.4, we describe various attacks over patient health information outsourced to the third-party service provider. Section 7.5 describes various encryption techniques used to maintain the security and privacy of EHR distributed to the cloud. Moreover, it provides a comparison between various encryption techniques. In Section 7.6, we provide recent developments to maintain the security and privacy of EHR outsourced to the third-party service provider.

7.2 **Existing technology**

Advancement in information and communication technology allows data collected and stored in one system is accessible throughout the world on demand. This can be done using the paradigm of cloud computing. EHR is outsourced to the cloud to provide on-demand global healthcare delivery.

7.2.1 *Cloud computing*

The definitions of cloud computing are as per the following:

According to Buyya *et al.*

“A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service level agreements established through negotiation between the service providers and consumers” [12].

According to NIST

“Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [13].

The paradigm of cloud computing has been proposed with various service-oriented models. They incorporate infrastructure as service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The service provider bestows platform, infrastructure, and software which can be accessed by cloud computing users. It provides unlimited storage and computing resources. There are many commercial cloud computing systems developed by Information technology industries. Example of such systems is Amazon’s EC2, IBM’s Blue Cloud, and S3, Yahoo Pig, Google APP engine, and customer relation management system

salesforce. The huge preferences of cloud computing paradigm are it is quick and straightforward to send, adaptable, scalable, unlimited data storage, high resiliency, secure against network attacks, fast accessing, cost-effective, efficient, fast recovery in case of disaster, and real-time detection of system tampering. These benefits help health service providers to use the paradigm of cloud computing to store and access the patient's EHR. Figure 7.1 shows the users of EHR outsourced to the cloud. The users of EHR outsourced to the cloud are patients, patient's family members, medical professionals, pharmacists, hospital management, and insurance providers.

In addition, Figure 7.2 demonstrates the working of a cloud-based EHR framework. In spite of all these benefits, there are security concerns over the data outsourced to the cloud, which short its usage. Most of the cloud-based EHR system is patient-centric to bestow data privacy. The patient has full control over his

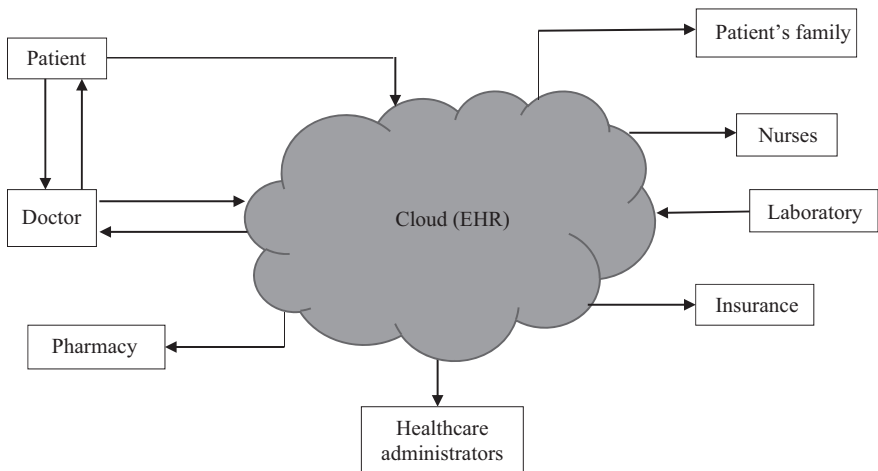


Figure 7.1 Users of cloud-based EHR

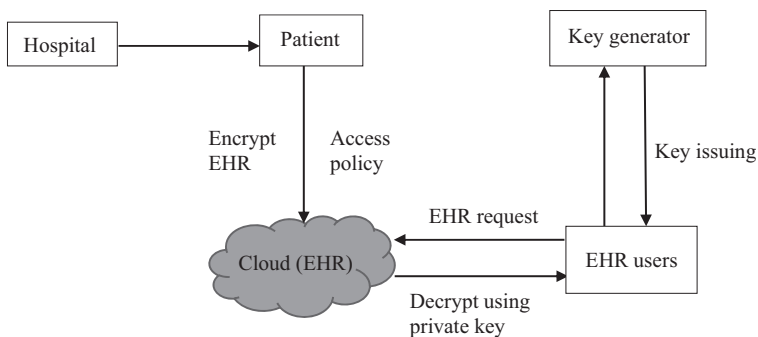


Figure 7.2 Cloud-based EHR system

EHR. For each encounter with medical professionals, the patient's medical record is updated. The patient encrypts his EHR and imposes access control policy over EHR. Then the patient outsources his EHR to the cloud. The decryption process can be done when the user receives a key from the key generator. The user key has to match the access control policy to decrypt EHR.

7.2.2 Fog computing

As wireless body area networks (WBAN) attracted medical industry in capturing and monitoring patients, cloud computing falls to satisfy certain requirements [50]. The major drawback of cloud computing is that the network might cause overload [14,46]. In addition to this, there is a delay in rendering information to the end users. This may result in late treatment to the patient. So fog computing is employed to overcome the drawbacks of cloud computing [15]. Fog computing the term was coined by Cisco in 2014, and it is defined as a distributed, decentralized network where resources are stored between cloud and end user. Fog computing thus reduces the distance in the network that the data must be transmitted. Fog computing has the advantages of providing closer proximity to end users, consuming network bandwidth, enhancing response time, and improving data security. This is achieved by localizing the computation that is the computation is done in local area networks. In fog computing, there is an additional layer in between the cloud and the source of data. Thus it decides which data can be processed locally and which data has to be sent to the cloud. The drawback of fog computing is it is less scalable and little expensive.

7.3 Security requirement for EHR

Data privacy and security should be ensured before EHR is outsourced to the cloud [49]. Health Insurance Portability and Accountability Act of 1996 (HIPPA) provide EHR security regulations to provide effective healthcare delivery to patients [16]. The following are the security requirements needed to protect EHR outsourced to the cloud from unauthorized access.

7.3.1 Data integrity

The data entered in EHR should be accurate, relevant, and complete. As the data are interchanged between many users, the data may be changed, or there may be a documentation error. Alternatively, the hackers intentionally change the report of a patient. Data integrity alludes to shielding information from unauthorized access, so each transaction should follow atomicity, consistency, isolation, and durability [17].

7.3.2 Interoperability

Health records stored in one system should be accessible in another system is called interoperability [18]. Achieving interoperability is very important to provide effective healthcare delivery for patients, to improve workflow, and to reduce ambiguity. EHR outsourced to the cloud should provide proper communication and cooperation between the authorized users.

7.3.3 Data privacy

Data privacy refers to the longing of an individual to control the revelation of his personal data. Patient's medical record includes more confidential data such as the patient's disease, drug usage, financial condition, and sexual preferences. If this sensitive data are disclosed, there may be a change in the patient's life. Technically and financially, the patient may have to face the loss. Patient's record ought to be unveiled distinctly with the authorization of the patient. So the patient's EHR ought to be shielded from indecent exposure [19,20]. Data privacy has to be maintained by hiding the data using robust encryption techniques.

7.3.4 Fine-grained access control

Every one of the users of EHR has various roles: for example, a doctor, a patient, medical attendants, and lab expert. Each user performs a different task and has different responsibilities. So they should be given access to specific information according to their role and responsibilities [21]. They should not access all the information on the patient's medical record. For example, a lab technician should only be allowed to insert lab reports in medical records.

7.3.5 Availability

Availability refers to EHR ought to be available upon interest by an approved user [22]. System availability incorporates a systems capacity to carry on activities notwithstanding when a few authorities act mischievously. Moreover, the system must be able to proceed with activities even there is a security rupture. The information should be accessible whenever it is necessary.

7.3.6 User privacy

User privacy refers to the access of EHR only to the authorized users. In several encryption schemes, the key issuing authority can access all the messages under the user private key. User privacy has to be maintained to resist key escrow problem [23].

7.3.7 Scalability

Scalability is the ability to extend the EHR by adding resources. EHR outsourced to the cloud should provide scalability concerning key management, computation, user revocation, and storage [24].

7.3.8 User revocation

User revocation is if the attributes of the user become invalid, the user access to EHR should be revoked [25]. The user no longer can access the EHR. So EHR outsourced to the cloud should ensure on-demand user revocation to maintain data integrity. The security model corresponding to user revocation has referred to forward secrecy.

7.4 Attacks over EHR

In spite of the benefits of storing medical records electronically, it also serves as a repository for hackers. Patient's identification record and health record transmitted over the insecure channel are subjected to several attacks. These attacks could result in low quality of health service to patients. The global information gives an estimation that the health care records worth ten times more than the credit card number [2].

7.4.1 Destruction and modification

Destruction and modification attack made in the system or when the data flow through the network. Destruction is the attacker destroy specific or complete information from the record. A modification is changing the information found in the record [26]. These attacks result in inaccuracy in medical records, which leads to wrong treatment for the patient. There is a loss in the security requirement data integrity.

7.4.2 Denial of service

The attacker performs several tasks, such as generating lots of meaningless messages and send to the authorized user. Alternatively, the attacker may block the file needed for the target authorized user. So the authorized user is denied to access the resources that are needed to perform a task in the electronic health record [26].

7.4.3 Disclosure

Patients may not wish to reveal their personal data such as religion, HIV diagnosis, a genetic condition, sexual orientation, and reproductive health that may result in personal embracement and damage to personal reputation [20]. Disclosure refers to the unauthorized reading of stored information [26]. This attack may occur during data transformation as well as within the system.

7.4.4 Repudiation

Repudiation attack is an authorized user request for a task and finally denies that he didn't make the query. This attack may also occur at the receiving side that the receiver denies that request hasn't received in spite of receiving the request [26].

7.4.5 Masquerading

The adversary goes about as an approved user to access the information despite the fact that the attacker is not an approved user [26].

7.4.6 Insider attack

An insider attack is finished by the workers of an organization who have genuine access to their organization's data. They utilize their organization's Information technology infrastructure to submit misrepresentation [27]. The real insider attack

occurs after the worker is ended from the organization. The workers of the organization may not pursue the guidelines constantly.

7.4.7 Spoofing attack

There are three types of spoofing attack [28]. They are IP address spoofing attack, address resolution protocol (ARP) spoofing attack, and domain name system (DNS) server spoofing attack. In the IP address spoofing attack, the attacker launch IP packets from the different source address to overload the network traffic. This results in the denial of service attack. In ARP spoofing attack, the attacker links his/her MAC (Media Access control) address with authorized user IP address. In DNS server spoofing attack the attacker reroutes the domain name to the different IP address in order to launch viruses.

7.5 Maintaining security and privacy of EHR in existing technologies

By encrypting EHR and by user authentication, the privacy and security of EHR are maintained. The encryption technique used to protect EHR should satisfy the above-explained security requirements, and it should be efficient. The various encryption techniques used to encrypt EHR and authentication techniques is described below in detail. The various advantages and disadvantages in each encryption techniques and authentication techniques are also discussed in this section.

7.5.1 Symmetric key encryption

Also known as single key encryption is symmetric key encryption. Because both the sender and the recipient concur with a single private key. This single secret key is used to encrypt and decrypt. The sender and recipient should keep this secret key secure, and the adversary should not be aware of this secret key [29]. Only the secret key is kept secure, the encryption and decryption algorithm is not kept secret. The encryption and decryption algorithm is known publicly. The definition of symmetric key encryption mathematically is as follows.

A symmetric-key encryption took the form of a map $E: K \times M \rightarrow C$, so that the map $E_k: M \rightarrow C, m \rightarrow E(k, m)$ is referred to as encryption function for each $k \in K$.

$D_k = E^{-1} k$ is referred as the decryption function.

The stream ciphers and block ciphers are examples of symmetric key encryption. Sharing of secret key between both the sender and the recipient is a risky task in maintaining the security in symmetric key encryption. According to Shannon secret key sharing, the output of a good cipher should be confused and diffused. Confusion means hiding the local patterns from the attacker. Diffusion means the ciphertext formed from the plaintext should mix around different parts such that nothing remains in its original place. According to Shannon, a good cipher should be substitution and transposition. The public key encryption scheme can accomplish this secret sharing of the key. In addition to secret key sharing between sender and receiver, there are many advantages to symmetric key encryption. Because

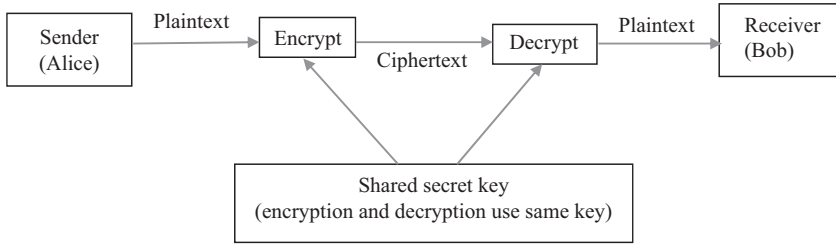


Figure 7.3 Symmetric key encryption

symmetric key encryption uses a large key size, it is safe against attack by brute force. Moreover, in both hardware and software, it can be implemented efficiently because it generates strong keys. Figure 7.3 shows the symmetric key encryption function diagram.

Using user biometrics, modern symmetric key encryption generates the secret key. Biometrics are transformed into a template that can be cancelled and then shared between the sender and the receiver. It is possible to use symmetric key encryption in EHR encryption. Numerous work used symmetric key encryption for encrypting EHR [30–32]. Speaking about the applicability of symmetric key encryption in encrypting EHR is not convenient. Because the secret key should be shared between the doctor and the patient. So if a doctor has n patients, the doctor has to maintain n keys. Moreover, a doctor has to communicate with other doctors regarding patient conditions, with the pharmacy regarding drugs and many more, so each party in the whole system has to maintain many numbers of keys which is very difficult.

7.5.2 Public key encryption

Two separate keys are used to encrypt and decrypt a message in order to avoid using the same key for encryption and decryption. The encryption key is publicly available, and the receiver keeps the decryption key secret. When the receiver able to decrypts the message, but not by the opponent, the data confidentiality is achieved. Diffie and Hellman implemented first public key encryption. Diffie and Hellman proposed that the sender and recipient perform some private mathematical computation on their side and achieve a shared secret key to exchange messages. This is called a Diffie–Hellman key agreement (DH-KA) [33]. Figure 7.4 shows the functional diagram of public key encryption.

Public key encryption (PKE) scheme security is based on the assumed problem of hard mathematical computation. However, a man in the middle attack happens in PKE. The adversary may modify the sender's messages by pretending that the adversary is the original sender to the receiver. Having a trusted third party called certificate authority to issue the certificate to the public key can solve this man in the middle attack. The sender receives the receiver's public key and certificate and verifies the public key. If the verification process succeeds the sender use receivers

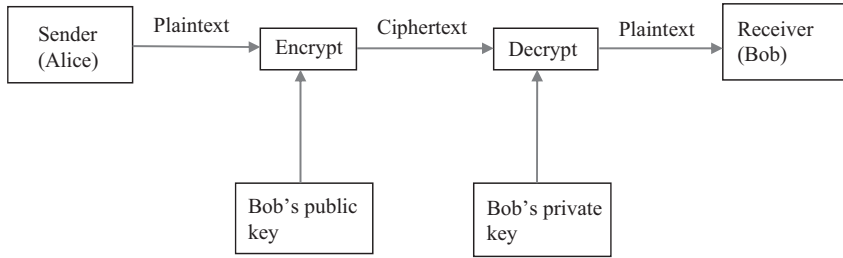


Figure 7.4 Public key encryption

public key to encrypt the messages. The major drawback of certificate authority PKE is to maintain the certificates which are complex and cumbersome. Public key encryption is employed in encrypting EHR in these works [34,35].

7.5.3 Identity-based encryption

To overcome the certificate management in PKE, Shamir in 1984 introduced identity-based encryption (IBE) [33]. The user's public key is an arbitrary string that is a user identifier rather than a number. For instance, the e-mail address may be the identity of the user. The sender with the recipient's email address encrypts the messages and sends them to the recipient. A trusted third party called a private key generator (PKG) generates the users' private key. Both the sender and the receiver must authenticate to PKG in order to obtain their private key that corresponds to their identity [33]. Figure 7.5 illustrates the identity-based encryption function diagram.

For encrypting her, IBE [36] can be used, but the main drawback is when a patient enters a hospital without conscious, he may not be able to say his identity. Speaking about the security of IBE it suffers key escrow problem and the communication between the PKG and the users should be secure to transfer private key.

7.5.4 Attribute-based encryption

Amit Sahai initially introduced attribute-based encryption (ABE) as Fuzzy identity-based encryption [45]. ABE's primary notion is to provide tolerance for errors. ABE uses a set of attributes to identify the user. Each message is encrypted using a set of attributes. Therefore, a ciphertext is not connected to a single user. When users attributes match the attributes of ciphertext, the user can decrypt the ciphertext. Key ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE) have been developed to ensure fine-grained access control over ciphertext by the researchers. Access policies are associated with user decryption key in KP-ABE, and the ciphertext is associated with the set of attributes. The ciphertext can only be decrypted by users if the ciphertext attributes satisfy the key policy. In CP-ABE, the ciphertext is linked to access policies, and the user decryption key is formed using the set of attributes. Users can decrypt the ciphertext only if the key-related attributes satisfy the ciphertext-related access policy. The access policy is a monotonic tree structure. Figure 7.6 shows an example of the access structure.

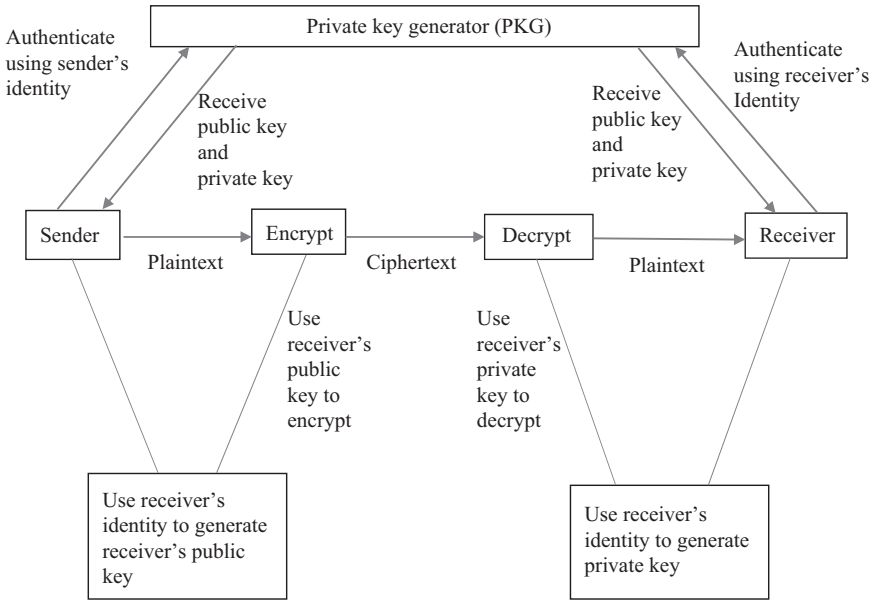


Figure 7.5 Identity-based encryption

KP-ABE was first employed by Yu *et al.* [7]. The disadvantage of the Yu *et al.* scheme is that it lacks flexibility in managing attributes and lacks scalability in employing various levels of attribute authorities. In addition, the data owner must have complete confidence in the key issuing authority in KP-ABE, since the data owner can only select the attributes associated with the ciphertext. Key issuing authority enforces access control policies related to user keys. KP-ABE is therefore not suitable for EHR encryption. However, in describing the data owner's access control policies, CP-ABE deployed by Bethencourt *et al.* [37] is well adaptable. However, satisfying the modern business environment is not enough because it does not support complex, flexible, and efficient policies on access control and management of attributes. When complex access control policies are imposed, ABE suffers from inflexibility. In addition, the ABE scheme requires the data owner of EHR to maintain all the attributes that are burdensome in a single authority. The data owner may not be in a condition to maintain all the attributes which lack scalability.

7.5.5 Multiauthority attribute-based encryption

Multiple attribute authorities overthrow the drawback in the single authority ABE scheme. ABE multiauthority is classified as ABE multiauthority with a central authority and without a central authority. Chase proposed the first multiauthority system with a central authority [38]. The owner of the data selects a set of attributes and number nk and encrypts the message to create the ciphertext. Where n is the

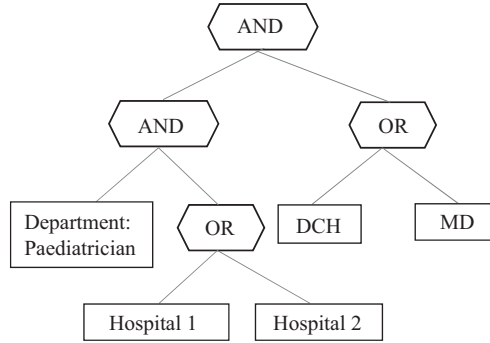


Figure 7.6 Tree access structure

number of authorities, and k is the number of attributes that a user must meet to receive part of the decryption key for each authority. Each attribute authority holds a separate set of attributes. The user must submit attributes to authorities if the number of attributes k is satisfied the user receives part of the private key from each authority. The primary challenge faced by Chase was to prevent the collision. He prevented the collision by having a global identifier (GID) for each user. Every user must submit his GID to the central authority in order to collect part of the key other than from authorities. The users should combine all the keys received from the authorities and from the central authority to form the decryption key. In addition, to decrypt the message, the user must satisfy the minimum number of attributes. The authorities can join together in a central authority scheme to form the private key of users. By adopting multiauthority ABE without a central authority introduced by Chase and Chow [39] the above-said shortcoming is overwhelmed, and user private key is generated by the authorities using pseudorandom functions. The authorities are resisted from knowing GID of the user by adopting an anonymous key issuing protocol.

Many research work to secure outsourced EHR to the cloud has been published. Li *et al.* developed KP multiauthority ABE to secure the scalability, user privacy, and fine-grained access control of HER [24]. Moreover, KP-ABE is not suitable for encrypting EHR because the data owner has no rights to enforce access policies over his data. So there is a breach of data privacy. So Qian *et al.* [9] modified Li *et al.* work to CP multiauthority ABE. Both divided the users of the system into public and private domains. Public domain users are medical professionals, and private domain users are patient and his family members. Data owner itself manages the attributes of private domain users. However, maintaining attributes of public domain users is difficult for the data owner, so multiple authorities maintain user attributes in the public domain. The drawback of these schemes is the public key of the users has to be transferred through a social network. So there is complexity in issuing keys to the users. The framework of these schemes are shown in Figure 7.7.

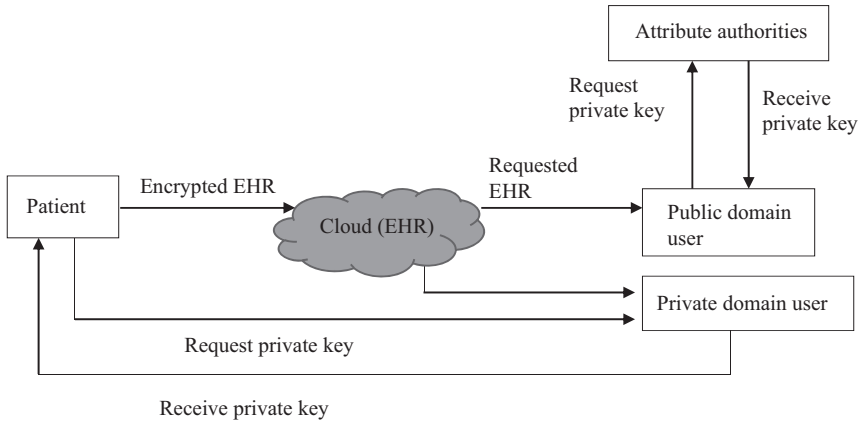


Figure 7.7 The framework of Li *et al.* multiauthority ABE scheme

7.5.6 Hierarchical attribute-based encryption

Hierarchical ABE was developed by Wang *et al.* [40] as a combination of hierarchical identity-based encryption and CP-ABE. Fine-grained access control over EHR outsourced to the cloud is approved in this scheme. The hierarchical structure to the cloud users is provided to make the encryption scheme more efficient. The hierarchical ABE architecture is depicted in Figure 7.8.

The root authority acts as a PKG in hierarchical ABE, which configures system parameters and generates keys for top-level domain authorities. Domain authority generates keys for authorities or users of the next level. The leftmost second-level domain authority in Figure 7.8 maintains all users and other authorities by maintaining a disjoint subset of attributes. This scheme provides cloud providers with fine grain access control and full delegate access. The drawback of this scheme is when the same attribute has to be maintained by multiple domain authorities that is impractical when certain complex policies are imposed. Moreover, attributes cannot hold multiple values, but in a real-world scenario, a single attribute may hold multiple values for an individual user.

7.5.7 Attribute set based encryption

A set of attributes are associated with the user decryption key in CP-ABE. CP-ABE doesn't support effective user attribute management as a result of the users will solely use all doable combos of attributes to satisfy the tree access policies. In addition, for the same attribute, CP-ABE does not support multiple values. In a real-world scenario, a particular attribute hold multiple values. In EHR, an individual has multiple diseases, so the attribute disease holds multiple disease values. An attribute-based encryption scheme (ASBE) was introduced by Bobba *et al.* [41]. He introduced key structure to users, which is a recursive attribute set. In CP-ABE each element of user key is an attribute, but in ASBE, each element of user key

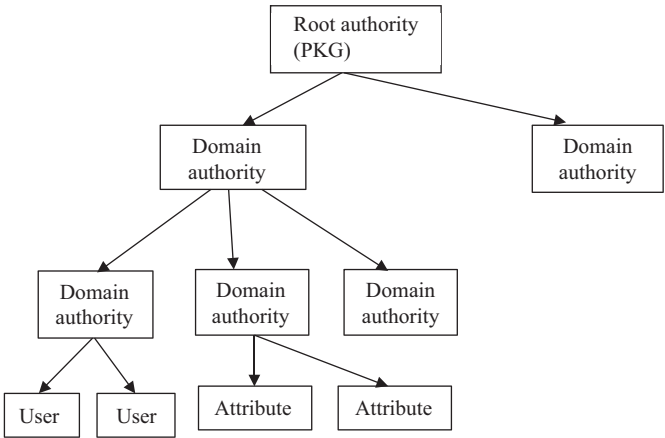


Figure 7.8 Architecture of hierarchical ABE

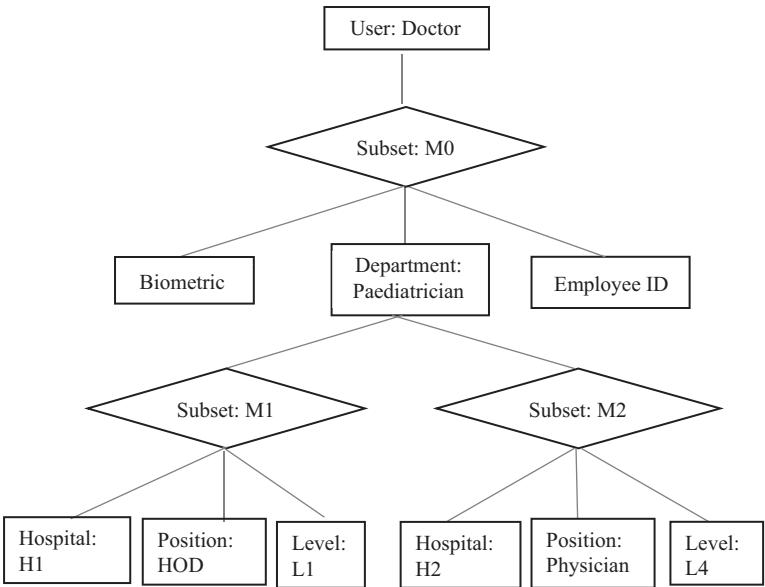


Figure 7.9 Example key structure

comprises of either attribute set or an attribute. This allows users to combine multiset attributes to meet the access policy embedded in the ciphertext. An example of a key structure is shown in Figure 7.9. As CP-ASBE does not support multiauthority scheme, so there is a breach in user privacy. Managing keys by a single authority are cumbersome.

Figure 7.9 shows depth 2 key structure explains a doctor working in hospital H1 and H2, and he is working as HOD in H1 and physician in H2. Thus it allows multiple values for each attribute for a single person. ASBE ensures greater flexibility by enforcing dynamic constraints in combining attributes to satisfy the ciphertext-related tree access structure.

7.5.8 Hierarchical attribute set based encryption

Hierarchical structures are adapted to the system users in the hierarchical attribute set based encryption (HASBE). This scheme is a combination of hierarchical ABE and ASBE. HASBE provides EHR outsourced to the cloud with scalability, flexibility, and fine-grained access control. Figure 7.10 shows the hierarchical structure of system users.

There are five types of system users in this scheme. They are a cloud service provider, trusted authority, domain authority, data owner, and data users. Various levels of domain authorities are there in this scheme. Top level domain authorities are managed by a trusted authority. Other domain authorities are maintained by its parent domain authority. The domain authority manages all EHR owners and EHR users. This explains the system users' hierarchical structure in the HASBE scheme [4]. The owner of the EHR outputs his EHR, which is encrypted into the cloud. The data users receive from the cloud service provider the requested encrypted file. Only when the key received from the domain authority meets the

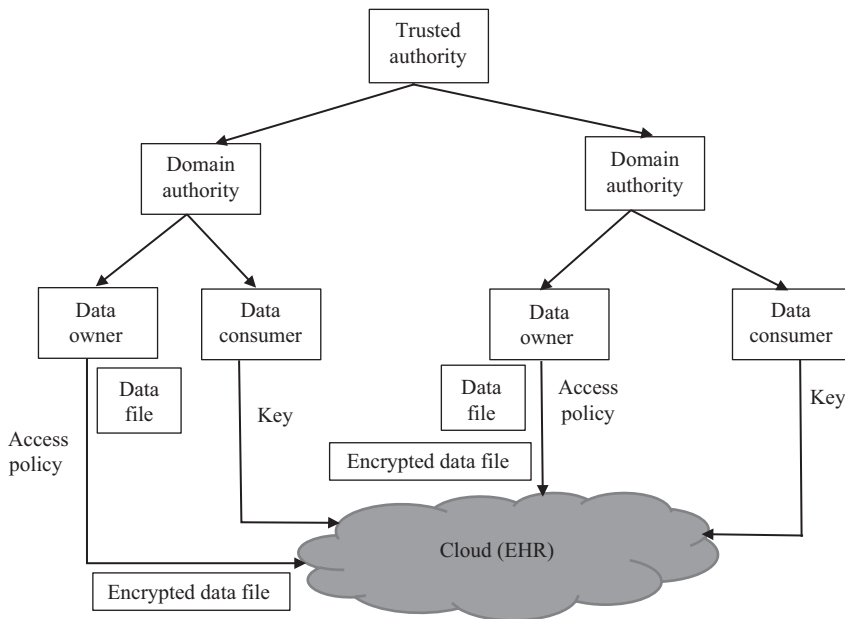


Figure 7.10 Architecture of HASBE

access policy enforced by the data owner, then the data user can decrypt the encrypted file received from the cloud.

When it comes to the security requirement that this scheme satisfies, it is more scalable, more flexible, and provides more fine-grained access control compared to previous encryption schemes. Moreover, it provides effective user revocation by adding expiration time in the decryption key of the user. This expiration time indicates the period of the key is valid. After the expiration time, the user key is not valid to decrypt the EHR outsourced to the cloud. The shortcomings of this scheme do not provide write access control. This scheme does not satisfy the security requirement data integrity, which is crucial. User privacy is not maintained because the user has to trust the domain authority who issue keys. Moreover, there is also a breach of data confidentiality because users can collide together to access the sensitive data file beyond their access privilege.

7.5.9 *Comparison of various encryption techniques*

In this section, we compare the various encryption techniques used to encrypt EHR outsourced to the cloud. In terms of interoperability, availability, scalability, and fine-grained access control, symmetric key encryption falls according to the comparison. In addition, key management is inefficient. Public key encryption falls in scalability, interoperability, data privacy, data integrity, and user privacy. It is also inefficient in key management and key distribution. Speaking about the applicability of public key encryption for EHR, it is very difficult to adopt because of the complexity in expanding and key management. Identity-based encryption also falls with the same drawbacks found in public key encryption except there is no cumbersome in maintaining certificates for the public key. Speaking about single authority ABE key management and distribution is difficult.

In addition, KP-ABE is not well suited to encrypt EHR because the data owner cannot define the policy of access control over his EHR even though it provides fine-grained access control. CP-ABE with single authority provides privacy of data and user revocation complexity is reduced. Multiauthority ABE schemes reduced the complexity of key management and key distribution. It provides scalability, user revocation, and fine-grained access control, but data privacy is infringed as the data owner has to rely on third party attribute authorities. In order to increase scalability, flexibility, and fine-grained access control, hierarchical ABE schemes are adopted. It provides system users with a hierarchical structure. However, data integrity and privacy are lacking. To meet the real world scenario that user attribute may hold more than a single value attribute set based encryption scheme is adopted, this provides more flexibility fine-grained access control compare with other encryption techniques. The comparison of different encryption techniques is shown in Table 7.1.

7.5.10 *Various authentication schemes*

Authentication also helps to maintain EHR's privacy and security, which is outsourced to the cloud. Authentication is classified as data authentication and user

Table 7.1 Comparison of various encryption techniques

	Symmetric key encryption	Public key encryption	Identity-based encryption	KP-ABE	CP-ABE	Multi authority ABE	Hierarchical ABE	ASBE	HASBE
Key management	Difficult	Difficult	Difficult	Difficult	Difficult	Moderate	Moderate	Moderate	Efficient
Certificate management	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Key distribution	Hard	Hard	Hard	Hard	Hard	Easy	Easy	Easy	Easy
Scalability	No	No	No	Difficult	Difficult	Yes	Yes	Difficult	Yes
Data integrity	Yes	No	No	No	No	No	No	No	No
Data confidentiality	Yes	No	No	No	Yes	No	No	No	No
User privacy	Yes	No	No	No	No	No	No	No	No
Fine-grained access control	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Availability	Yes	No	No	No	No	No	No	Yes	Yes
Interoperability	No	No	No	No	No	No	Yes	Yes	Yes
User revocation	Hard	Hard	Hard	Hard	Hard	Moderate	Moderate	Efficient	Efficient
Man in the middle attack	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flexibility	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Applicability	No	No	No	No	Moderate	Yes	Yes	Yes	Yes

authentication. Authentication of data is the process that ensures the source of the data. Authentication of the user is the process to ensure the authenticity of the user. Digital signature schemes, login/password with a digital certificate, username/password, password/PIN, smart card/PIN, smart card authentication, and biometric-based authentication schemes are various authentication techniques used to secure EHR outsourced to the cloud [42]. In this section, we discuss these authentication techniques briefly.

7.5.10.1 Digital signature schemes

Many researchers have developed digital signature schemes to secure EHR based on public key infrastructure. Digital signature schemes are used for data authentication [48]. The user authentication process consists of two keys which bounds to the user's identity. Certificates for the user's key has to be maintained, which is cumbersome and costly. So certificate less digital signature schemes are developed by adopting hierarchical identity based digital signature schemes. Comparing with all digital signature schemes, biometric-based signature schemes [51] provide stronger security by avoiding man in the middle attack.

7.5.10.2 Username/password

User authentication scheme mostly uses username/password mechanism to secure EHR. However, it does not meet the security requirement needed for EHR. This mechanism does not guarantee data integrity as a man in the middle attack is susceptible. It is also possible for password sharing, cracking, and copying if debuggers and disassemblers are used.

7.5.10.3 Password/PIN

This Password/PIN mechanism also does not provide adequate security to EHR outsourced to the cloud. This mechanism is also prone to man in the middle attack thus a breach in data integrity. Password and PIN can be lost or stolen.

7.5.10.4 Login/password with digital certificate

To improve the security of EHR, there should be another factor, including the password. So HIPAA regulation advice two-factor authentication. So login contains the username or email address anything identifying the user. Along with it, a digital certificate is needed for the user to prove his authenticity. Biometrics of user can be used instead of the digital certificate to improve the security of EHR.

7.5.10.5 Credential system

In this authentication scheme, a trusted third party will issue credentials to the users. The user holding legitimate credential can access the EHR outsourced to the cloud. This scheme bestows more security compared with previous schemes.

7.5.10.6 Smart card based authentication schemes

Smart card based authentication scheme is also employed by several researchers to maintain the privacy and security of EHR [32]. A smart card, including token and

PIN, is widely used for securing EHR. However, the main drawback is the authentication of the token provider. An adversary can issue token for the user so that there is a breach in the security of EHR. Moreover, there is a chance for token missing or theft.

7.5.10.7 Biometric-based authentication

Biometric-based authentication provides stronger security for EHR outsourced to the cloud [52]. It avoids man in the middle attack. By employing biometric, certificate management is avoided. There are also security issues in employing biometric. Recent research says biometric can be reframed from the minutiae [42]. So employing biometric template in smart cards are risky.

7.5.10.8 Comparison of various authentication schemes

Table 7.2 shows the comparison of various authentication schemes used to protect EHR. Looking at different authentication schemes utilized for verifying EHR outsourced to the third party service provider password/Pin based confirmation plot is powerless against be stolen by enemies. In credential based verification conspire the client hosts to believe the third party, giving the qualifications. Two-factor authentication scheme such as smart card alongside token furnishes greater security contrast to the password-based framework. However, the enemy can go about as a token supplier and issue token to the client. This outcome in high danger of information breach. Contrasted with all other authentication biometric-based authentication demonstrated to be increasingly secure. As it is a physical attribute, the client need not recollect it. Data integrity is guaranteed in biometric-based authentication. The downside of biometric-based authentication is it costly to keep up and to actualize. These days geographic authentication is additionally utilized, as shown in Table 7.2.

7.6 A recent development to maintain privacy and security of EHR

We discuss various solutions in this section to protect data privacy, user privacy, and data security in EHR. Cloud-based EHR provides limited data integrity. There is no auditing system to check the user who accesses the EHR. Data integrity can be improved by having user biometric as one of the attributes and having a biometric-based server sided authentication scheme. The solution above improves the integrity of data and shields from man in the middle attack. User privacy in a single attribute authority scheme is complicated. In multiauthority schemes, user privacy is improved. However, providing data confidentiality is very difficult because EHR is under the control of many authorities. These authorities can collide together to access the EHR outsourced to the cloud. Cloud-based EHR requires the patient to trust the service provider and attribute authorities, even though EHR is encrypted prior to outsourcing.

The transactions should be transparent and traceable in order to maintain EHR's privacy and security outsourced to any third-party service provider.

Table 7.2 Comparison of various authentication techniques

	Digital signature	Username/ password	Password/ PIN	Login, password and digital certificate	Credential system	Smart card	Biometric based
Brute force attack	No	Yes	Yes	Yes	Yes	No	No
Man in the middle attack	No	Yes	Yes	No	No	Yes	No
Cost	Moderate	Less	Less	Moderate	Less	Expensive	Expensive
Maintenance	High	Less	Less	High	High	Less	High
Convenience	No	Yes	Yes	No	Yes	Yes	No
Confidentiality	Yes	No	No	No	No	Yes	Yes
Privacy	Yes	No	No	No	No	No	Yes

Transaction histories should be maintained so that the patient can know who accessed his EHR. In the cloud computing paradigm, unauthorized access to EHR is cut down by having proper access control mechanisms but tracing the user who accessed the EHR is difficult.

7.6.1 *Blockchain technology*

Recently blockchain technology replaced the paradigm of cloud computing. Blockchain can be implemented for scattered computing resources. Therefore it is well suited in storing and accessing patient health information [43,47]. The data flow diagram of EHR stored in the blockchain storage network is shown in Figure 7.11. The process involved in storing EHR in the blockchain is explained below.

- Upon each encounter of a patient to medical professionals, the medical professionals store the EHR locally and send it to blockchain client.
- The blockchain client encrypts the EHR with patient's public key.
- Then the encrypted EHR is transmitted to the blockchain storage network together with metadata.
- All other access points in the blockchain network check the accuracy of the changes.
- If other access points accept the change, EHR is transmitted to the public ledger.
- The users of EHR can download it from the public ledger and decrypt it using patient's private key.
- The patient can download his EHR anywhere and anytime from the ledger and share it with other health professionals.

MedRec is a blockchain system mainly used for accessing patient healthcare information [44]. This system provides an immutable log to the patients and provides access to EHR of patients to health service providers. MedRec allows patients to authorize new members to access his EHR securely. To provide secure access to EHR outsourced to blockchain MedRec follows authentication, confidentiality, accountability, and interoperability. Data integrity in the MedRec system is maintained by using a cryptographic hash function over EHR to resist tampering. It provides peer to peer communication, so there is no need for third party approval to access the EHR. It is patient-centric to have full control over his EHR by tracing the client who accessed his EHR. Moreover, it secures the EHR of the patient lifetime.

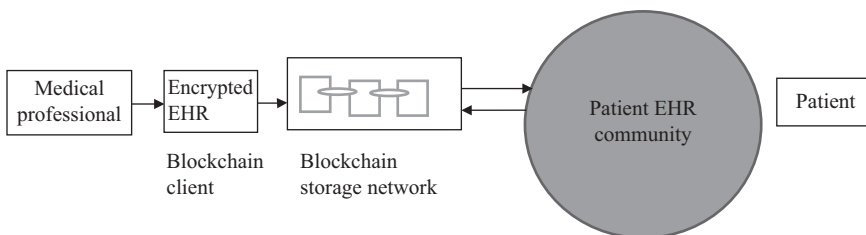


Figure 7.11 *Data flow diagram of EHR in blockchain network*

7.6.2 Advantages of blockchain over EHR

In this section, we describe the advantage of adopting blockchain to store and access the health information of a patient.

1. EHR contains patient sensitive data storing in trusted third party arises many security issues. As blockchain paradigm does not force data owner to trust the third party data privacy is improved.
2. Blockchain does not force the user to trust the third party, and it involves only peer to peer communication thus it maintains user privacy.
3. As blockchain is decentralized approach patient can encounter his health check-up anywhere and anytime. The patient does not want to go for following to the same health center to maintain his EHR.
4. EHR of the patient is easily accessible by other medical professionals in case of emergency.
5. The patient can easily trace the user who accessed his EHR, so he has full control over his EHR.
6. EHR stored in blockchain is accurate because transaction histories are maintained, and it is transparent to other users.

7.6.3 Comparison of cloud computing and blockchain

In this section, the two paradigms are compared to where EHR is stored and accessed. Comparing with the cloud computing paradigm, the blockchain paradigm provides more security to EHR. The paradigm blockchain provides data integrity, accuracy, and data confidentiality. Moreover, it resists insider attacks by providing traceability and auditable of transaction histories.

However, the blockchain paradigm does not provide flexible access control over EHR. The user can provide EHR with a hierarchical structure in cloud computing and enforce access control policies across each medical record in order to provide fine-grained access control. The paradigm of blockchain provides flexible computation over scattered data so it would be most adaptable in healthcare service environment if it also provides fine-grained access control over EHR. The comparison between existing cloud-based EHR and blockchain based EHR is shown in Table 7.3.

Table 7.3 Comparison between cloud computing and blockchain technology

	Cloud computing	Blockchain
Central node	Yes	No
Trusted third party	Yes	No
Computing resources	Compute centralized data	Compute decentralized data
Database	Centralized	Decentralized
Communication	Server-based communication	Peer to peer communication
Traceability	No	Yes
Auditability	No	Yes
Data integrity	No	Yes
Accuracy	No	Yes
User privacy	No	Yes
Fine grained access control	Yes	No
Insider attacks	Yes	No

7.7 Conclusion

The paradigm of cloud computing and fog computing is the existing technology to store and access EHR. It is a significant concern to maintain EHR privacy and EHR security outsourced to the cloud service provider. Currently, security issues are reduced by encrypting EHR and enforcing access control policies before it has been outsourced to the third party storage. We discussed several encryption techniques for encrypting EHR in this chapter. The encryption scheme should be efficient, and it should satisfy the security requirement needed to protect EHR from unauthorized usage. Most of the encryption schemes do not provide data integrity. To ensure data integrity, each transaction in EHR should be transparent, auditable, and traceable. Using the paradigm of cloud computing, data integrity cannot be achievable. In cloud computing, the owner of the EHR must trust attribute authorities or the cloud service provider to store his EHR. It may lead to a lack of data privacy. Moreover, in the real-world scenario, the patient may go to a different hospital as he moves from one place to another, leaving his record scattered. Using the cloud computing paradigm, this scattered data cannot be accessible. These cloud computing deficiencies are being overthrown by emerging blockchain technology. In blockchain technology, each transaction in EHR is transparent, auditable, and traceable; thus, it provides data integrity. Using blockchain technology, scattered data can be maintained lifetime. Moreover, it does not force anyone to trust anybody. Thus it maintains data privacy and user privacy. Although blockchain technology offers many advantages over cloud computing, it does not provide fine-grained control of access over EHR. In blockchain technology, only the patient's private key can decrypt the encrypted EHR.

References

- [1] Stausberg J., Koch D., Ingenerf J., and Betzler M., "Comparing paper-based with electronic patient records: lessons learned during a study on diagnosis and procedure codes," *Journal of the American Medical Informatics Association*, 10(5), (2003), pp. 470–477.
- [2] Akpan N., "Has health care hacking become an epidemic?" February 2015. PBS News Hour.
- [3] Bahga A., and Madisetti V.K., "A cloud-based approach for interoperable electronic health records," *IEEE Journal of Biomedical and Health Informatics*, 17(5), September 2013.
- [4] Wan Z., Liu J., Robert H., and Deng D., HASBE: "A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, 2012, 7(2), pp. 743–54.
- [5] Sun J., Zhu X., Zhang C., and Fang Y., "HCPP: cryptography based secure EHR system for patient privacy and emergency healthcare," *In 2011 31st International Conference on Distributed Computing Systems*, MDPI, Minneapolis, MN, pp. 373–382.

- [6] Goyal V., Pandey O., Sahai A., and Waters B., "Attribute-based encryption for fine-grained access control of encrypted data," In *Proceedings of the 13th ACM conference on Computer and communications security*, ACM, Alexandria, Virginia, USA, October 30–November 3, 2006, pp. 89–98.
- [7] Yu S., Wang C., Ren K., and Lou W., "Achieving secure, scalable, and fine-grained data access control in cloud computing," In *2010 Proceedings IEEE INFOCOM*, San Deigo, CA, March 15–19, 2010, pp. 1–9.
- [8] Alshehri S., Radziszowski S.P., and Raj R.K., "Secure access for healthcare data in the cloud using ciphertext-policy attribute based encryption," In *2012 IEEE 28th International Conference on Data Engineering Workshops*, IEEE, Arlington, VA, USA, 2012, pp. 143–146.
- [9] Qian H., Li J., Zhang Y., and Han J., "Privacy preserving personal health record using multiauthority attribute-based encryption with revocation," *International Journal of Information Security*, 2015, 14(6), pp. 487–497.
- [10] Hayrinen K., Saranto K., and Nykanen P., "Definition, structure, content, use and impacts of electronic health records: a review of the research literature," *International Journal of Medical Informatics* 77(5), (2008), pp. 291–304.
- [11] Ekblaw A., Azaria A., Halamka J.D., and Lippman A., "A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data," In *Proceedings of IEEE Open and Big Data Conference*, IEEE, Vienna, Austria, August 13, 2016 (Vol. 13, pp. 13).
- [12] Mell P., and Grance T., "NIST definition of cloud computing," *National Institute of Standards and Technology*. Special Publication 800-145, October 7, 2009.
- [13] Wang G., Liu Q., and Wu J., "Hierarchical attribute based encryption for fine-grained access control in cloud storage services," In *Proceedings of the 17th ACM conference on Computer and communications security*, ACM, Chicago IL, USA, October 4–8, 2010, pp. 735–737.
- [14] Kumari A., Tanwar S., Tyagi S., and Kumar N., "Fog computing for Healthcare 4.0 environment: opportunities and challenges," *Computers & Electrical Engineering*, 72, 2018, pp. 1–13.
- [15] Hathaliya J., Tanwar S., Tyagi S., and Kumar N., "Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach," *Computers & Electrical Engineering*, 76, pp. 398–410, 2019.
- [16] 104th United States Congress. Health Insurance Portability and Accountability Act of 1996 (HIPPA). Online at <http://aspe.hhs.gov/admnsimp/pl104191.htm>, 1996.
- [17] Bowman S., "Impact of electronic health record systems on information integrity: quality and safety implications," *Perspectives in Health Information Management*, 2013,10 (Fall), ncbi.nlm.nih.gov
- [18] Jardim S.V.B., "The electronic health record and its contribution to health-care information systems interoperability," *Procedia Technology*, 9, (2013), pp. 940–948.
- [19] Harman L.B., Flite C.A., and Bond K., "Electronic health records: privacy, confidentiality, and security," *AMA Journal of Ethics*, 2012, 14(9), pp. 712–719.

- [20] Omotosho A., and Emuoyibofarhe J., "A criticism of the current security, privacy and accountability issues in electronic health record," *International Journal of Applied Information Systems (IJ AIS)*, 7(8), 2014, pp. 11–18.
- [21] Wang G., Liu Q., and Wu J., "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," In *Proceedings of the 17th ACM conference on Computer and communications security (ACM CCS)*, ACM, Chicago, IL, 2010, pp. 735–737.
- [22] Fernandez-Aleman J.L., Señor I.C., Lozoya P.Á., and Toval A., "Security and privacy in electronic health records: a systematic literature review," *Journal of Biomedical Informatics* 46(3), 2013, pp. 541–562.
- [23] Narayan S., Gagne M., and Safavi-Naini R., "Privacy preserving EHR system using attribute-based infrastructure," In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, ACM, Chicago, Illinois, 8 october 2010, pp. 47–52.
- [24] Li M., Yu S., Zheng Y., Ren K., and Lou WL., "Scalable and secure sharing of personal records in cloud computing using attribute based encryption," *IEEE Transactions on Parallel and Distributed Systems*, 2012, 24(1), pp.131–43.
- [25] Wang G., Liu Q., Wu J., and Guo M., "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Computer & Security*, 30(5), pp. 320–331.
- [26] Win K.T., Susilo W., and Mu Y., "Personal health record systems and their security protection," *Journal of Medical Systems*, 2006;30(4), pp. 309–15.
- [27] King J., Smith B., and Williams L., "Modifying without a trace: general audit guidelines are inadequate for electronic health record audit mechanisms," In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, ACM, Miami, Florida, 28–30 January, 2012, (pp. 305–314).
- [28] Ekblaw A, and Azaria A. MedRec: Medical data management on the blockchain. *Viral Communications* [Internet]. 2016 Apr 11; Available from: <https://viral.media.mit.edu/pub/medrec>
- [29] Delfs H., and Knebl H., 2002. *Introduction to Cryptography* (Vol. 2). Berlin: Springer, pp. 11–31,
- [30] Ueckert F., and Prokosch H.U., "Implementing security and access control mechanisms for an electronic healthcare record," In *Proceedings of the AMIA Symposium*, American Medical Informatics Association, PMC, 2002, pp. 825–829.
- [31] Jian W.S., Wen H.C., Scholl J., *et al.* "The Taiwanese method for providing patients data from multiple hospital EHR systems," *Journal of Biomedical Informatics*, 2011, 44(2), pp. 326–332.
- [32] Yu W.D., and Chekhanovskiy M.A., "An electronic health record content protection system using SmartCard and PMR," In *2007 9th International Conference on e-Health Networking, Application and Services*, IEEE, Taipei, Taiwan, 19–22 June 2007. pp. 11–18.
- [33] Chatterjee S., and Sarkar P., "Identity-based encryption," Springer Science & Business Media; 2011, Springer Publishing company.

- [34] Zhang R., and Liu L., "Security models and requirements for healthcare application clouds," In *2010 IEEE 3rd International Conference on cloud Computing*, IEEE, Miami, Florida, 5–10 July, pp. 268–275.
- [35] Sun J., and Fang Y., "Cross-domain data sharing in distributed electronic health record systems," *IEEE Transactions on Parallel and Distributed Systems* 2009, 21(6), 754–764.
- [36] Boldyreva A., Goyal V., and Kumar V., "Identity-based encryption with efficient revocation," In *Proceedings of the 15th ACM conference on Computer and communications security*, ACM, Alexandria, Virginia, USA, October 27–31, 2008, pp. 417–426.
- [37] Bethencourt J., Sahai A., and Waters B., "Ciphertext-policy attribute based encryption," In *Proceedings of IEEE Symposium on Security and Privacy 2007 (SP'07)*, IEEE, Oakland, California, USA, 20–23 May, 2007, pp. 321–334.
- [38] Chase M., "Multi-authority attribute based encryption," In *Proceedings of the 4th Theory of Cryptography Conference (TCC'07)*, Amsterdam, The Netherlands, February 21–24, 2007, pp. 515–534.
- [39] Qian H., Li J., Zhang Y., and Han J., "Privacy preserving personal health record using multiauthority attribute-based encryption with revocation," *International Journal of Information Security*, 2015, 14(6), pp. 487–497.
- [40] Chase M., and Chow S.S.M., "Improving privacy and security in multi-authority attribute-based encryption," In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09)*, Chicago, Illinois, USA, November 09–13, 2009, pp. 121–130.
- [41] Buyya R., Yeo C.S., Venugopal S., Broberg J., and Brandic I., "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, 2009, 25(6), pp. 599–616.
- [42] Rezaeibagha F., Win K.T., and Susilo W., "A systematic literature review on security and privacy of electronic health record systems: technical perspectives," *Health Information Management Journal*, 2015, 44(3), p. 23.
- [43] Bobba R., Khurana H., and Prabhakaran M., "Attribute-sets: a practically motivated enhancement to attribute-based encryption," In *European Symposium on Research in Computer Security*, pp. 587–604. Springer, Berlin, Heidelberg, 2009.
- [44] Drew I., "Moving toward a blockchain-based method for the secure storage of patient records," In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST, August 2016.
- [45] Sahai A., and Waters B., "Fuzzy identity based encryption," In *Proceedings of Advances in Cryptology–Eurocrypt*, Aarhus, Denmark, May 22–26, 2005, vol. 3494, pp. 457–473.
- [46] Vora J., Tanwar S., Tyagi S., Kumar N., and Rodrigues J.P.C., "FAAL: fog computing-based patient monitoring system for ambient assisted living," *IEEE 19th International Conference on e-Health Networking, Applications*

- and Services (Healthcom-2017)*, Dalian University, Dalian, China, October12–15, 2017, pp. 1–6.
- [47] Vora J., Tanwar S., Verma J.P., *et al.*, “BHEEM: a blockchain-based framework for securing electronic health records,” In *IEEE Global Communications Conference (IEEE GLOBECOM-2018)*, Abu Dhabi, UAE, December 09–13, 2018, pp. 1–6.
- [48] Vora J., Devmurari P., Tanwar S., Tyagi S., Kumar N., and Obaidat M.S., “Blind signatures based secured e-healthcare system,” *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, July 11–13, 2018, pp. 177–181.
- [49] Vora J., Italiya P., Tanwar S., *et al.*, “Ensuring privacy and security in e-health records,” *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, July 11–13, 2018, pp. 192–196.
- [50] Tanwar S., Thakkar K., Thakor R., and Singh P.K., “M-Tesla-based security assessment in wireless sensor network,” *International Conference on Computational Intelligence and Data Science (ICCIDS 2018)*, NorthCap University, Gururgram, India, April 07–08, 2018.
- [51] Tanwar S., Obaidat M.S., Tyagi S., and Kumar N., Chapter 10: “Online signature-based biometrics recognition,” M. S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG, 2019, pp. 255–285.
- [52] Tanwar S., Tyagi S., Kumar N., and Obaidat M.S., Chapter 21: “Ethical, legal, and social implications of biometrics technologies,” M.S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG, 2019, pp. 535–568.

Chapter 8

Healthcare models and algorithms for privacy and security in healthcare records

*Bandana Mahapatra¹, Rajalakshmi Krishnamurthi²,
and Anand Nayyar³*

With the ever-increasing cost of healthcare and premium healthcare insurance, there is a significant need for proactive healthcare and wellness. Considering the present status of clinical records, most of the records are maintained on legacy paper-based file management systems which is not only expensive, but also unsecure, as sometimes, record leakage or sometimes some disasters can spoil the records of patients. So, it is highly recommended that medical records should be shifted from paper-based legacy old system. In recent times, the new wave of digitizing medical records has seen a paradigm shift in the healthcare industry. And medical industry is rapidly implementing electronic health records (EHR) systems. With EHR systems, numerous benefits will come in terms of cost control, quality improvement, sales promotion of evidence-based medicine, record keeping, security, and high mobility. So, EHR systems should be designed and tailored in such a manner to meet with metrics and requirements in terms of data completeness, failure resistance, availability, and high security.

Beside certain challenges which surround EHR systems like funding, technology, attitude, and organizational aspects, healthcare-based IT industry is still growing at whooping rate to provide quality ICT services to hospitals, medical practitioners, and patients. Many hospitals are adopting to healthcare IT solutions to stand ahead of other competing healthcare organizations. However, IT support for healthcare industry is quite challenging and complex as it comprises of fusion of lots of ICT technologies like mobile computing, Internet of Things, Cloud Computing, and Big data. Although, healthcare IT system has several new opportunities for competitive advantages, there are some serious security and privacy concerns need to be addressed. Data Security is the central point of concern to be concentrated upon, as data have to be safe, secured, and transferred in an encrypted manner from remote locations to central database management systems operational

¹Department of Computer Science and Engineering, Dhole Patil College of Engineering, Pune, India

²Department of Computer Science and Engineering, Jaypee Institute of Information Technology, Noida, India

³Graduate School, Duy Tan University, Da Nang, Vietnam

at remote data centers. Apart from security, data privacy is also an important criteria that needs to be worked upon so as to ensure that only authorized personal should be able to access the healthcare records.

The objective of this chapter is to discuss three major approaches, namely Data Storage, Data Access, and Data Authentication with regard to electronic healthcare records so that patient's records are kept safe and follow Confidentiality, Integrity, and Availability principle. The chapter also focuses on the various algorithms that are connected to above three approaches with regard to maintaining security and privacy in healthcare IT.

Key contributions of this chapter are as follows:

1. Discussion of security related aspects in healthcare.
2. Highlights working of various healthcare models implementing security and privacy in healthcare.
3. Discussion regarding algorithms used for data storage and access with regard to security and privacy.

8.1 Introduction to data security in healthcare

The evolution of IT sectors has contributed immensely in the growth and development of various fields enhancing the quality of lifestyle maintained by the people. Be it electronic devices of medical science or field of aerospace engineering, information technology and its emergent field can be seen as being applied as a construct in some way or the other. With the accelerating demanding of IT, the organizations have moved from paper-based health records into Electronic Based Health Records System (EHRs) revolutionizing the entire healthcare industry. The various healthcare proposals have claimed that integration of health records into the organization has proved to be enormously beneficial such as it reduces cost, improves quality of care, record keeping, promotion of evidence-based medicine, mobility, etc. Figure 8.1 shows the various data and services provided by an Electronic Health Record System to a Healthcare Organization [1].

The advent of modern advancements in ICTs and digital management of healthcare records has made us reach to a position where patients' health data are facing new security and privacy threats. The security system can be expressed in terms of confidentiality, integrity, and availability (CIA). The protection and security of personal information a vital aspect in the health sector, and hence makes it mandatory for developers to ensure the CIA of personal health information. As per the ISO EN13606 standard, confidentiality is defined as the "process that ensures weather information is accessible only to authorized users." Integrity is defined as to assure that information is correct and is not tampered by any unauthorized user. The integrity of health records is utmost priority to ensure the safety of patient's health and to ensure that the information's entire life cycle is fully auditable making it mandatory for software development firms to use various models to implement healthcare security [2].

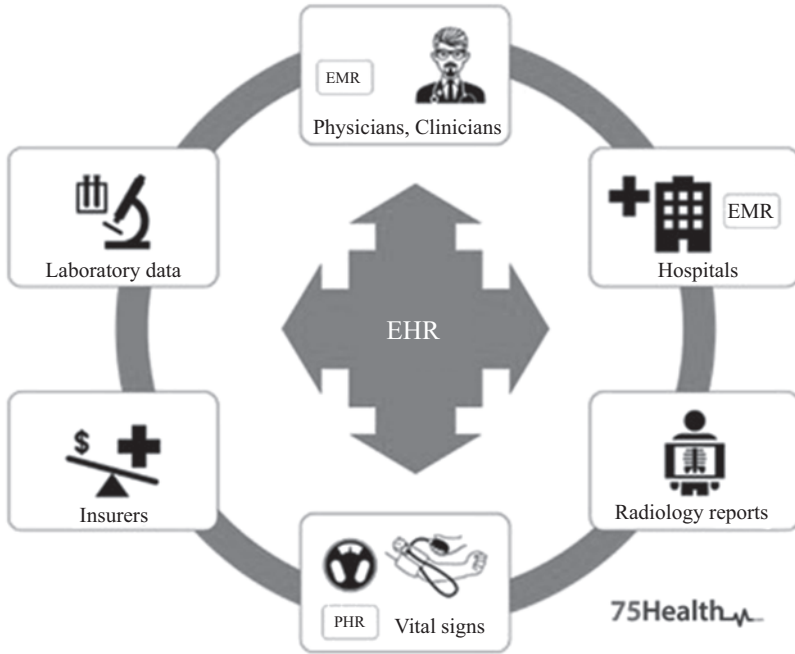


Figure 8.1 Data and services recorded in EHR [1]

As we know healthcare-based IT industry is growing at a whopping rate to provide quality Information Technology services to hospitals, medical practitioners, and patients, many hospitals are adopting to healthcare IT solutions to stand ahead of other competing healthcare organizations. However, IT support for the healthcare industry is quite challenging and complex as it comprises of fusion of lots of ICT technologies like IoT, Big Data, Cloud Computing, and Wireless Body Area Networks [3–10]. Although, healthcare IT system has several new opportunities for competitive advantages, there are some serious security and privacy concerns need to be addressed. Data security is the central point of concern to address as data have to be safe and secure and transferred in an encrypted manner from remote locations to central database management systems operational at remote data centers. Data privacy also needs to be addressed as only authorized persons are required to access the healthcare records.

A designed EHR system is required to satisfy certain requirements such as data completeness, resilience to failure, high availability, and consistency of security policies in order to offer its benefits to the organization [1,2].

The major issues that need to be worked upon in forming an electronic based health record system are funding, technology, attitude, and most prominently organizational aspects. However, very limited development has been made on the policy development aspects related to privacy concerns highlighted by a move from largely disconnected paper-based health record system into an integrated, electronic

based Health record system [1]. The blooming in areas of information and communication technologies has placed us in a situation where the patients' health data are facing new challenges pertaining to the security and privacy issues. The health information is considered as one of the most crucial as well as critical to the healthcare industry that is susceptible to serious threats like hackers, viruses, and worms which calls for the need to have a robust security mechanism designed for maintaining the security of privacy of the electronic health records of healthcare organization.

The fundamental security requirement of EHR systems is confidentiality, integrity, and availability which needs to be considered while designing a security model for a given healthcare organization.

The upcoming sections in the chapter discuss the various healthcare security models and algorithms that are being used as well as have been proposed to ensure they meet the security as well as the privacy concern of the organization [11]. The chapter is organized as follows: Section 8.2 provides an overview on the healthcare, its evolution as well as security aspects; Section 8.3 discusses about the security issues that needs to be addressed in an EHR system belonging to any healthcare providing organization; Section 8.4 examines the detailed study of various models conceptualized to implement the security aspects in an EHR; and Section 8.5 covers the algorithms proposed, adopted as well as implemented in order to ensure a secured EHR system. Sections 6–8 describe the data storage security, data access security, and authentication mechanism, respectively. Section 8.8 concludes the paper.

8.2 Healthcare overview

The concept of healthcare security has various contrasting and divergent interpretations made at different platforms like United Nations Development Program (UNDP) or World Health Organization (WHO), etc. The fundamental role of a security in the healthcare stream is into protection against attacks causing threats to various public health approaches with respect to operational implications of individual or a community level [11].

8.2.1 Healthcare evolution

The major heritage in the area of hospital security can be found in Great Britain. The first organizational hospital facility was seen in United Kingdom at St. Bartholomew Hospital at Smith's Field in London in 1123 where the hospital was granted a royal charter by King Henry VII in 1546. Thereafter, in 1552, house of governors authorized "the order of the hospital" to be implemented which is currently termed as a job description. This marked the start of a concept of healthcare security.

Early healthcare centers in UK were functioning under the board of governors till 1948. Thereafter the Department of Health and Social Security was formed and thereafter Social Security Act came into effect [12].

The Security Development philosophy has been changing with era as follows:

- 1900–1950: the security was all about protecting the hospital.
- 1950–197: the security or “Hospital Protection” concept included aspects of law.
- 1960–1975: the hospitals became aware of other security aspects apart from fire hazards and illegal activities.
- 1975–1990: the day to day functioning of security expanded.
- 1990–Next century: rapid changes have occurred integrating new concepts like risk management, IT blooming, EHR systems, organization of healthcare, etc.

8.2.2 Healthcare information security

The concept of information security primarily deals with the aspects of protection enforcement toward information and information system from illegal access and use, disclosure, disruption, alteration, deletion, etc. The information security can be achieved by ensuring criteria’s like confidentiality, integrity, and availability of information [12,13].

- Confidentiality—the criteria states that health information should remain confidential and should not be accessed by unauthorized personnel.
- Integrity—the criteria states that health information should not be tampered or deleted by any outside person.
- Availability—the criteria states that health information should be available to access only by an authorized person.

8.2.3 Need to implement privacy in healthcare data and information

Currently the healthcare systems are majorly dependent on the technology, be it hardware, software, medical devices, or sensors for sending, storing, and retrieving data. Here the health informatics play a crucial role in the healthcare industry, making it much more efficient. But the cyber threats make the technology unreliable to depend upon, hence, making way for healthcare security enforcement. The

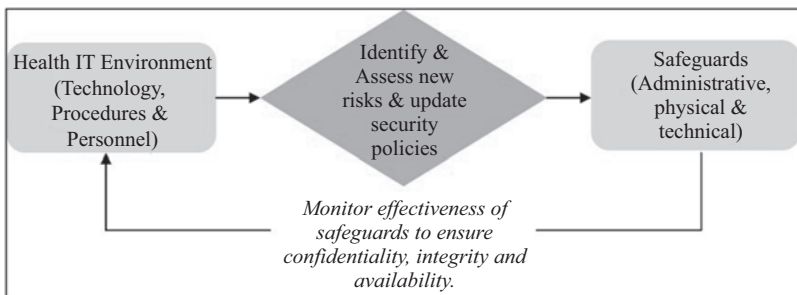


Figure 8.2 An example to implement security in Healthcare IT environments [12]

cyber security is quite important to both the people as well as the healthcare industry. Criminals may use leaked information to sell on the black market, which may be used for crimes like identity theft, Medicare fraud, or other financial gains. The prevention of cyber-attacks may also keep patient information keep confidential, which is required for legal reason. The security enforcement also prevents the leakage of patient information which saves them from being convicted by law firms [13].

8.2.4 Health security as a public health concept

The concept of healthcare security is being widely accepted by the general mass. But the definitions related to the concept of health security with respect to public health operational terms are insufficient reconciliations of the health security concept with community based primary healthcare. Moreover, there are wide gaps in the basic concept and its usage in various scenarios [13,14]. The policy makers in an industrialized country put stress over the protection of their population, especially against the external threats like terrorism or pandemics, while healthcare workers and policy makers belonging to a developing country or United States have a broader perspective of the concept defined in public health. The concept again has a varied use when comes to United Nation (UN) agencies, for example, WHO has its own restrictions in usage of the term “global health security.”

8.3 Security issues in healthcare data and information

Although technological advancements contribute in enhancing the quality of healthcare delivery, the beneficial attributes of these must be in a proportion to the privacy and the security aspects of the users. The in-home sensors, medical records data are transmitted electronically over the Internet through wireless transmission, which makes it all the more prone to danger of being compromised in both privacy and security aspects of individuals which are discussed as follows:

- Data access and storage
- Data mining
- Conflicting regulatory framework

A. Data access and storage—The aspect of confidentiality and privacy has always been a priority with respect to a patient health record [13]. Personal health being attached to the Internet has exposed confidential data to much more hostile forms of attack as compared to the paper based medical records. The patient today has to practically undergo a healthcare facility to get their medical records. As these records are majorly paper based, it physically restricts the number of people accessing the records and its transmission manner. The digitized form of data has paved the way for hackers and other malicious forms of attack to access the personal stored information as well as those having authorization. Moreover, the distributive nature of sensor networks, with respect to in-home patient monitoring

there is a huge challenge to enforce data security and integrity as compared to the traditional healthcare system. The varied attacks like eavesdropping and skimming area are possible during wireless transmission of sensor data. The data access storage and integrity are key challenges while implementing Electronic Patient Record (EPR's) and in-home sensor networks.

The regular queries related to challenges in electronic records and remote transmission of information needed to be answered are:

- Data ownership.
- Data type.
- Storage of healthcare data.
- Viewers of the medical records of patients.
- Right to view the records irrespective of the patient's consent.

Data ownership: The queries related to data ownership are: [11]

- *Who owns the data?*
- *Who holds the authority to perform actions like, delete, edit, and insert information to the health data as well as enforce regulations surrounding it?*
- *Whether patients own the data collected from testing them?*
- *Whether they are joint owners sharing the ownership?*

Data type: The queries related to data types includes kinds of data, quantity of data to be stored, for example, doctors' notes, MRI's, Lab Tests, etc. are few examples that are stored in the patients' paper-based records. Regarding EPRs the questions that arise are, will all the data be electronically stored or just a subset is sufficient enough for the healthcare purpose. The queries also apply with regard to the remote patient monitoring using sensor network, such as if the bulk data be stored locally at the patient's residence where the data pertaining to diagnosis and emergency response is transmitted back to the monitoring center. The quantity of sensor data deposited at the central location meets with the requirements to complete the patient care related tasks. Any related additional information may not hold significant impact over the patient care, but may add to the reason for being compromised in individual privacy. In both the cases the granularity of the data collected as well as stored requires to be reduced as much as possible while still achieving the required level of healthcare.

Data storage: The queries related to the data storage is mainly regarding the centralized versus decentralized storage. For example, queries are mentioned as follows:

- *Whether the data concerning EPRS should be stored in local database to facilitate interlinking or a central database repository system should be designed?*
- *Will the raw sensor data be stored locally or at a central monitoring station in case of a remote patient monitoring?*
- *What kind of data storage is perfectly suitable to maintain security issues and privacy needs of the user?*

Viewers of patient's medical records: The EPR users can be broadly segregated into the following categories:

- (a) Users having read/write privileges—Doctors, nurses, who can read, write as well as edit the patients EPR records.
- (b) Users with read privilege—Users of medical records like insurance providers are restricted only for viewing the patients EPR. Based on which user will be accessing the EPR further restrictions are applied to certain portions of the data.
- (c) Right to view records irrespective of patient's consent—There are certain scenarios where patient's information needs to be shared with people other than previously mentioned authorized users. For example, during emergency the reports may require its disclosure with certain healthcare without patient's consent in order to provide patient with necessary care.

B. Data mining—It is defined as the process for analyzing data to identify relationships. The patient's medical data are considered as one of the most challenging but also most rewarding among other biological data and analysis. The data mining concept on the human subjects can provide observations that may not be gained or easily extrapolated from animal studies, while mining over human data, there are some privacy and security issues which sets a restriction over the collection, distribution, and analysis that can be done. Currently large amounts of medical information is not stored electronically and hence cannot be mined [12,13]. Though the data mining implemented over the records have issues over security and privacy, the heterogeneous nature of the database and the hazard scatterings of the data throughout the medical care facility with no common format or principal of organization restrict what can possibly be done. As the EPRs become widely spread, healthcare organizations have databases that are a repository of the patient's information in a common computerized format. This data is possibly thereafter easily shared with the communication network, which may create a larger source of human medical data. Considering the increase in data availability, it is next important to access the role of data mining and how it is managed. Based upon the mining factor of patient's medical data, the profile can be easily classified into various categories based on age, gender, or disease leading to discrimination and exclusionary effect. Prior to the data mining activity being taken place, it's important to ensure the anonymity of data.

The anonymity of data can be enforced at multiple levels, for example, removing personal identifiers such as name, age, and social security number that make it all the more challenging to link data up to a unique individual. The uncorrelated data can be linked to a large subpopulation, for example, people of a certain gender/race. The appropriateness of the anonymity of a given data mining task must thereafter be evaluated leading to the specification regarding who can have access to the data at, and what level of anonymity leading to furthermore design complication or challenges [13,14].

C. Conflicting regulatory framework—There are quite a number of rules and regulations related to healthcare sector framed which includes the Federal Regulations of the American Health Insurance, Portability and Accountability Act

(HIPAA) (discussed in Section 8.4.10) as well as various state regulations. Though the regulations offer a framework of policy, they have to be adapted as EPRs where season plays a major role in changing the way healthcare is delivered [15].

HIPAA is a set of rules that is mandatory, followed by the healthcare providers ranging from doctors, hospitals, etc. The rules are designed to allow all the patients to be able to access their own medical records, correct errors, and have the right to get information regarding how their personal information is used or shared.

Apart from HIPAA the state also holds the right to form rules, how they would like the medical practitioner to function which is also clearly discussed in Health Privacy Projects [16,17]. As currently stated by many researchers and healthcare organizations, HIPAA rules may be treated as a baseline, that is, the minimum set of rules covering basic protections to the consumers whereas stronger or stringent state laws play the major effective role.

Solutions available to enforce healthcare security—Few existing solutions to previously discussed security issues are:

- (i) **Role-based access control model (RBAC)**—A major concern in managing large networks is with regard to handle security administration complexity [18]. The RBAC model or the role-based security is one of the dominating models in this field for handling advanced access control. The model helps in reducing both the complexity as well as the cost of the cost-security administration in a large network application. The RBAC model is discussed in greater details in the upcoming sections.
- (ii) **Encryption**—The encryption technique can be applied in order to ensure the data security as well as preventing attacks such as eavesdropping, skimming, etc., the encryption method can be accomplished in both the hardware as well as the software. To attain the highest form of data security it is always advisable to enforce encryption of both the forms. Various asymmetric and symmetric key algorithms can be applied to provide software encryption [19]. Pertaining to the areas of sensor network, tiny sec [16] has been specifically designed and applied in medical sensor systems in certain US Universities with strong encryption and authentication techniques.
- (iii) **Authentication mechanism**—The authentication mechanisms in security can be incorporated in order to ensure that data actually coming from the person/entity it claims to [20]. There are numerous authentication algorithms developed, for example, password protection, digital signatures, or challenging response, authentication protocol. Various energy efficient and security methods are designed for sensor networks, for example, hash function in tiny sec.

8.4 Models for healthcare security

The prevalent security measures are currently dominating the healthcare security aspect of RBAC model. Various up gradations over the RBAC have been proposed by researchers as well as in industry.

This section we will discuss the various healthcare security model.

8.4.1 RBAC healthcare model

The RBAC model addresses the authorization control requirement over objects. It builds the prototype by adding the maintenance and administration features of the group users that are authenticated with the same permissions or needs into roles. The users here can be recruited as the members of the specific role basing upon their responsibilities or corporate position which in due course can be reassigned into another role without causing an impact over the underlying access control infrastructure [1,2,21]. Here the administration allows the user to keep discretionary capabilities on the objects it owns. It also provides the permission to the system administrator for specifying the security policies which affects the users. The mode of grouping the users, offer additional security related advantages, for example, possible separation of privileges, duties, with respect to access position of users basing on the authorization. This characteristic of RBAC that possibly grants granularity is quite an attraction for the health information system environment where the objects, restrictions differs from organization to organization basing on their policies, professional ability, function of explicit information owner consent, etc.

The concept of RBAC was conceived in year 1992 and was published by NIST (US National Institute of Standard and Technology) in year 2000 [2]. It was later adopted and formally published as American National Standard Institute (ANSI) standard in 2004.

The RBAC model consists of core hierarchal, static, and dynamic mode of segregating duty, relations components where it was aimed to cope up with the single organization's security policy strategy [13].

With the help of core or flat functionalities, the permissions allotted to roles and bound to the user sessions where the authorization decisions are made by the process of object mapping. Figure 8.3 highlights the role structure for core RBAC model in a Healthcare Organization.

This activity is dynamically performed for each and every object resource in the system. In RBAC concept the need to repeat permission on various group is not

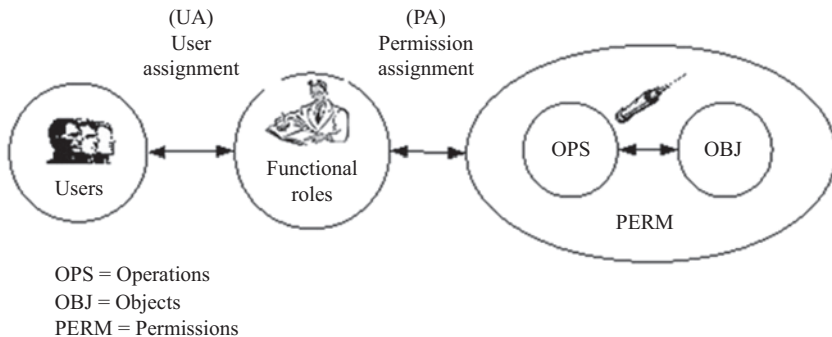


Figure 8.3 Role structure for core RBAC model [20]

required. Using hierarchy property one role can be connected to other associating constraints with permission sets. With the use of same token, various roles can be assigned to a single user. The relation established binds the users to his or her role and to his or her permissions [22].

Figure 8.4 shows the permission set existing between the various groups of users in a healthcare organization. The figure shows the medical directors, cardiologists, and rheumatologists sharing the doctors and resident's permission set. The cardiologists and the rheumatologists share specialist's permission.

The static or dynamic segregation of duty components can be availed to divide authority among various individual users to make the authorization criteria even straighter so that the prohibited activity is not possible alone by any single system user. The HIS may serve as an example for the environment that require stringent security over its various functionalities and information.

The healthcare industry present at various parks of the world uses RBAC massively over its system leveraging these properties. The RBAC capability to meet the health industry has become increasingly challenging with the enormous growth of technology like cloud computing, big data, data mining, etc., where the unpredictable scenarios continuously pose challenge's over the basic RBAC capabilities.

Various researchers have performed analysis over the RBAC to validate its security and efficiency. Lee *et al.* [21] used principle component analysis for collecting EHR access traffic over the network. They further suggest misuse detection over the network can be conducted by comparison of packages that need RBAC authority validation to be uniquely used in both x and y axis in comparison to a forged or attack package. Further, Helms and Williams also conducted an assessment of four different EHR RBAC aware system for the implementation cum evaluation where 25 attributes were selected with 8 being directly related to RBAC security. Their research showed the failure of all the systems trying to implement the RBAC component of separation of duties [20,22].

Taking into consideration the various healthcare systems scenarios with their limitations discussed through various approaches it can be enhanced into various

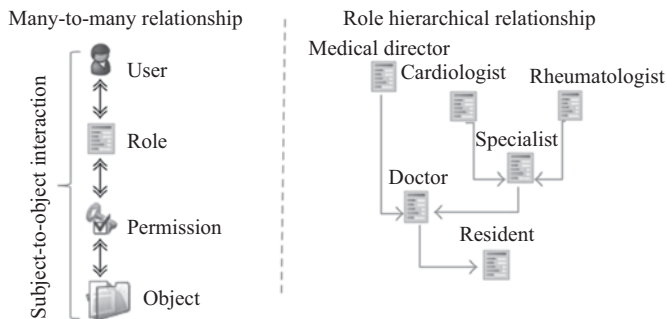


Figure 8.4 Permission sets existing between the various groups of users in a healthcare organization [16]

security trends addressed on RBAC aware HIS. Majority of the published articles do support RBAC adaptations, but have also mentioned areas of improvement on the current RBAC model in order to cope with diverse HIS implementations and its working scenarios such as

- *Conditional or emergency access and authorization delegation needs to be included.*
- *Context and situation access-based solutions should be supported by RBACs features that needs additional user obligations.*
- *The access segmentation and inter domain federation scenario is required.*
- *Record dependent or attribute-based encryption needs to be added using single or multiple trust supplier.*
- *Based on the highlighted limitations in the RBAC model various other healthcare models were proposed which are discussed below.*

8.4.2 Task role-based access control model

The proposed model is built upon RBAC designed considering the concept of task undertaking. The TRBAC model is primarily used in a healthcare environment in order to fulfil the management of access control. The TRBAC model is an improvement over an access control model which achieves its aim of access control through tasks. The model supports the dynamic real time security management. Here task may be defined as the basic unit of any healthcare activity [22,23].

In RBAC approach the permission is granted to roles, where the roles are assigned to users, whereas in T-RBAC the permission is delegated to tasks which are in turn handed over the roles. In T-RBAC model the users achieve permission of access control through roles. Here the medical tasks form the core component in the proposed healthcare system where they keep it functioning. Taking into account the main features of healthcare environment, T-RBAC model performs well, improving the managing capability of access control [21,24].

Figure 8.5 shows the T-RBAC modes for the user role task permission. The healthcare environment tasks can be classified into following four categories, depending on the task:

- Inheritable tasks
- Non-inheritable tasks
- Passive tasks
- Active tasks

	Non-inheritable	Inheritable
Passive access	A	B
Active access	Null	D

Figure 8.5 T-RBAC modes for the user role task permission

The concept of inheritable and noninheritable task is built on the structure of the medical organization. The model includes the role hierarchy where it has connection with the medical positions. In any given healthcare organization, a doctor is at a higher position compared to nurse, does not indicate that it can inherit full access rights from nurses. The T-RBAC partial inheritable access right from the lower medical positions [18,21].

The inheritable task indicates higher position inheriting from lower position and noninheritable task indicating the vice versa. The passive or the active task can be identified from the factor that it belongs to a working process or not. If the task belongs to a medical process it is an active access control or else it can be said as passive task.

8.4.3 HL7 role-based access control model

High level seven (HL7) basically offers a framework or standard for exchange, integration, sharing as well as retrieval of electronic health information. These standards specify the way information is packaged and communicated from one party to the other. HL7 standard supports clinical practice along with the management, delivery as well as evolution of health services which are recognized to be the most commonly used in the world [23].

The HL7 standards can be categorized into the following sections:

Section 1: Primary standards—Basic standards to specify system integrations, interoperability, and compliance.

Section 2: Foundation standards—Specify functional standards, tools, and building blocks required to build one standard.

Section 3: Clinical and administrative domains—The section states the documenting and messaging standards for clinical specialties and groups. These standards are generally implemented as soon as primary standards are established.

Section 4: EHR profiles—These standards offer functional models as well as profiles that enable the buildings for management of EHR.

Section 5: Implementation guides—This section discusses the implementation guides along with the supporting documents that are created to be used in conjunction with an existing standard. The documents existing in the section adds on as a supplement for the parent standard.

Section 6: Rules and references—The section relates to the technical specification, programming structures, along with the guidelines for software development.

Section 7: Education and awareness—The part carries the HL7's standard for trial use along with the current projects along with the various resources and tools that add on to supplement understanding and adoption of HL7 standards.

As we know RBAC serves as a means to control access to resources on an information system as was originally built to overcome the complexities attached toward managing individual user permissions and their assignments. The HL7 aims at simplifying authorization management, reduce administrative cost, improve

security, ease partner interoperability, establish new network level RBAC services, and improve service to members/clients/patients [24,25].

HL7 uses role engineering models in order to carry out their activities. Here models explain the relationships among components of an abstract role system to components of role engineering models.

The healthcare models are segregated into two levels:

- Functional roles
- Structural roles

The *structural role* defines the specified healthcare workflow that the users are allowed in taking part while the *functional roles* specifies the authorizations granted to entities in order to allow access to protected health information.

The HL7 role engineering process creates abstract healthcare work profiles, permissions and information model components. Using the model of RBAC, HL7 members identify and create tasks in order to drive abstract mission.

8.4.4 *Attribute role-based access control model*

The access-based access control model allows access to the various resources by subjects that can be determined by various attributes like name, IP address, time, etc. [15]. The model allows the authorization-based upon the various attributes [16]. The attributes play pivotal role in the process of granting permissions to the authorship users such as name, place, IP address, location, etc. The value attached to an attribute specifies in case a user is authorized to have a particular resource or not. ABAC is regarded as a flexible model which is considerably convenient to administer, provides ease of role structure, dynamic, and easy access control system for a given organization. Apart from these advantageous features the analysis of permission or change of user permission may be problematic or a difficult task in ABAC [14]. The ABAC model as shown in Figure 8.6 has ease of designing and role structuring, but is challenging in the case of analysis or management.

Coming to RBAC model, though it has ease of management and analysis of access control, but has a complex design with regard to role structure. Hence, considering lacunae in both the models, researchers suggested a hybrid model which can provide the advantages of both healthcare models, that is, RBAC and ABAC by keeping in mind their respective flaws and loopholes.

8.4.5 *Privacy access control model for e-healthcare service*

The various studies pertaining to the e-healthcare system has reported an additional threat that needs to be addressed is due to the systematic use of protected health information (PHI) raising threat to security, privacy as well as confidentiality to the e-patients information. For example, a US published survey reported, few citizens hesitate to file insurance claims or meet a healthcare provided with a fear of disclosure their health information might reduce their job prospects [26]. A user may also hold position in both primary as well as secondary user groups which pose an additional conflict, for example, cases where the doctor is being himself a patient. Figure 8.7 shows a primary access control model.

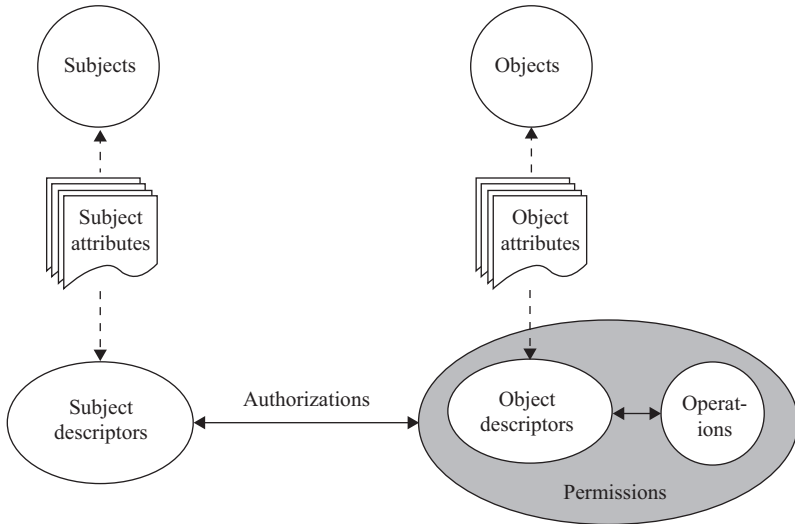


Figure 8.6. Design of attribute-based access control model

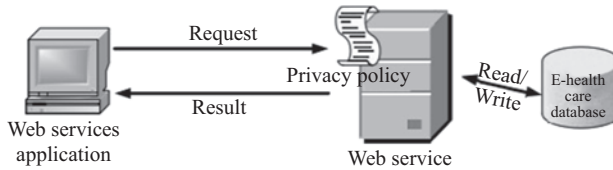


Figure 8.7 Working model of privacy control model for e-healthcare service

Considering the dynamic nature of e-healthcare services that makes the information access control a challenging task, RBAC model was proposed to be implemented for providing e-healthcare services. Here the core RBAC is presented as a set of criteria of use assertions with respect to users, roles, organizations, operations, and datasets. Here every data custodian has a user from an organization having at least one role assigned. The operations are thereafter allotted based on their roles for various job handling [26,27].

Figure 8.8 shows the privacy access control model with privacy extension designed over general RBAC

8.4.6 TMAC model

The TMAC model defined by Thomas [16] termed as team-based access control model to define the various roles of the users. The team role here is a set of rules specified within the team that constraints the role memberships. Team permission is a set of permission defined across team roles and objects. Here the context of team carries the user context as well as the object context. The proposed model by

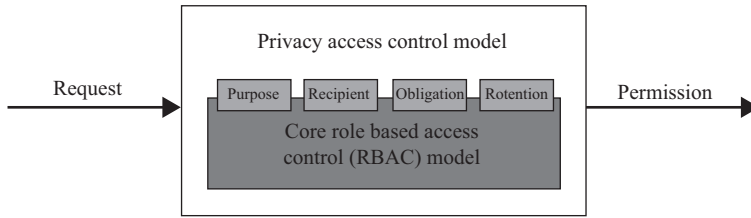


Figure 8.8 *Privacy extension over RBAC model*

Thomas has been further challenged by Wang stating it is unclear. The researcher has stated that TMAC does not provide an explanation on how to incorporate the team concept in RBAC framework. He further argues that the need of team roles as proposed in TMAC model is not required [27].

8.4.6.1 T-TMAC model

The T-TMAC model is based on the structure of the team organized and data exchange between them in a three-tier network. Here the scheduling has been arranged level by level where level 1 is among the medical nodes with associated coordinators level 2 between coordinators and video (v) level 3 is among video nodes and sink. The TMAC super frame follows the access methods replicating from IEEE 802.15.4 protocol with few modifications [25,26].

8.4.6.2 C-TMAC model

The model consists of five sets: role, user, context, permission, and session [2]. Here, a team is expressed as an independent entity which is used as intermediary in order to allow user access context. The team in the model is basically used as a context in order to group users for various roles to access other context that consists of some resources or environmental factors like time, location, etc. Here the users are assigned undeviated to teams on the basis of their organizational roles. Apart from its design shown in Figure 8.9, the model lacks explanation regarding its working details.

The model discussed user active security in order to limit access to specific objects based on factors like time and location.

8.4.7 *Security model for healthcare in cloud computing*

Cloud computing is defined as on demand, self-service Internet infrastructure to access computing resources anytime or anywhere [1]. It is a new model of delivering resources pertaining to the computation. The healthcare sector needs regular and constant innovations so as to remain cost effective, efficient, and fast in order to provide the high-quality services. Various researchers and industry experts predict that cloud computing concept is capable to change the face of health industry [16].

Many studies conducted or articles published stated the benefits of cloud computing proposing various models of framework with a view to improve the healthcare service [28–32].

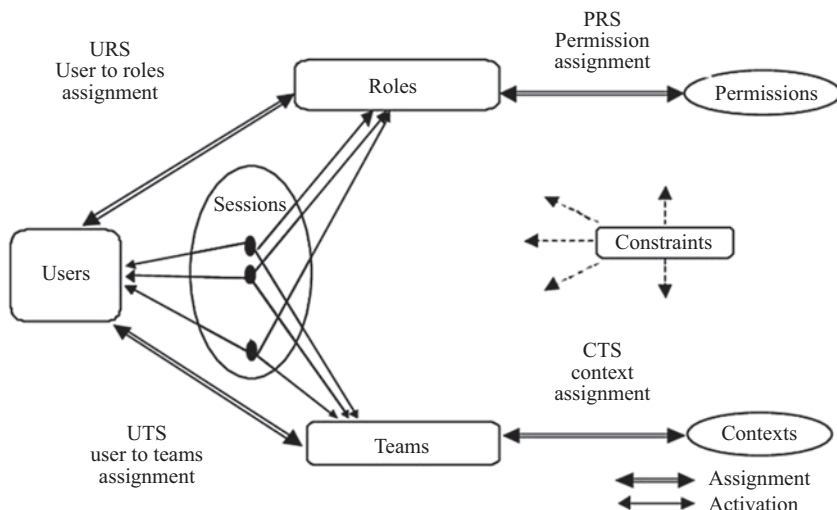


Figure 8.9 C-TMAC model design [26]

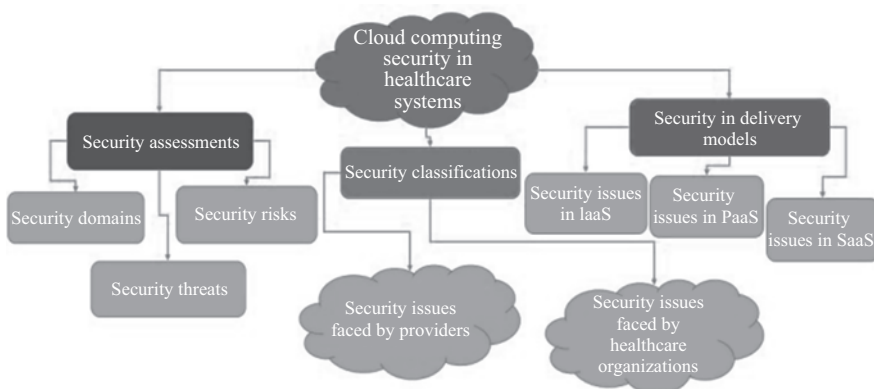


Figure 8.10 Security model design in cloud-based healthcare system [27]

Romalin *et al.* [33] proposed a cloud-based system to automate the process of collecting vital data from the patients from sensor network attached to medical devices and thereafter delivering the data to medical cloud for the purpose of storage and distribution as depicted in Figure 8.10.

The main attraction of this cloud-based system is that, it provides information to user's almost 7 days of the week. Its capability of real-time data collection removes the barrier to collect data manually with any possibility of typing error or even the deployment process [33].

Despite of its various benefits a strong resistance to adoption of cloud computing in healthcare is seen. The reason for the opposition centers is mainly on its

security concerns, though it claims to be secured enough in comparison to local household data. Various cloud providers have ensured a proper security mode like Microsoft, Google, Amazon, etc., the companies who have devoted huge resources in order to solve any security issues which local customers may not be able to afford.

Every security measure, if adopted on a large scale proves to be cheaper. Majority of cloud providers replicate the user data at various locations which leads to data redundancy and makes the system free from risk of system failure providing a method of disaster recovery. A cloud provider always has the ability of dynamic reallocation of security resources for filtering, traffic shaping, or encryption to increase the support of defensive measure. There are various data security risks like, hacker attacks, network breakers, natural disaster, separation failure, public management interface, etc. [27,28].

The cloud-based data are generally accessible to various customers, hence any provider failing to separate the resource may lead to serious problems. For example, request for data deletion may not exactly delete the data at multiple places where it has been stored rather is only made inaccessible. Such kind of data being accessed by third party customers in a cloud-based environment can impose huge risk.

The core mechanism of cloud computing system to guard against data loss and theft is strong encryption key management. However, a poor key management procedure may result in a loss of encryption keys or password to malicious parties or any unauthorized use for authentication.

8.4.8 *Security model for healthcare in big data*

As we know security can be specifically explained as the ability to preventing sensitive information about personal healthcare of a patient. The focus of all security enforcement is establishment of authorization with respect to accessing stored information in the system. The privacy aspect of the system also ensures that data collection, sharing, and utilization is performed in the righteous way [33,34].

The various technologies adopted to ensure security and privacy are:

- Authentication mechanism
- Encrypted data
- Access control
- Monitoring and auditing

Authentication: The authentication is a process of establishing or affirming weather claims made by an entity is true and authentic or not. The mechanism serves vital functions within an organization. Like a secured access to corporate networks, identity protection of users authenticates users that they are what they claim to be. This information authentication introduces further special problems such as man-in-the-middle attacks (MITM) [35].

Data encryption: Data encryption is considered as an efficient technique for preventing unauthorized access to sensitive data and even preventing an unauthorized access. The solution here protects as well as maintains the data ownership throughout its life cycle ranging from the data center to the end point which consists of mobile

devices used by physicians, clinicians as well as the administrators and into the cloud. The encryption mechanism is useful in order to eradicate exposure to breaches like packet sniffing theft of data from storage device, etc. The healthcare organizations need to ensure that the effective encryption scheme should be enforced, which should be able to use easily by both patients as well as the healthcare professionals as well as easily extensible to include new electronic health records.

Data masking mechanism: Data masking mechanism is termed as a methodology for replacing sensitive data elements with an unidentifiable value. It may not be considered as an encryption technique since the original value cannot be obtained from the masked value. Here the strategy used is deidentifying a data set or masking of personal identifier like name, social security number, or suppressing or generalizing quasi-identifiers like date of birth and zip code [36,37].

Access control: After the process of authorization the user may enter into an information system where the access is still controlled and monitored by the control policy which is designed basing upon rights of each practitioner authorized by the patient or an authorized third party which thereafter becomes a powerful and flexible mechanism to grant permission for users. It provides sophisticated authorization control in order to ensure that users can perform only the activities for which they have permissions like data access, job submission, cluster administration, etc.

Monitoring and auditing: The concept of security monitoring is about collecting as well as investigating the network events in order to catch an intrusion. The auditing mechanism records all user related activities pertaining to a healthcare system in a chronological order, for example, maintaining a record of events such an access to or modification of data. These two are a sort of optional security metrics which can be used to measure as well as ensure the safety of a healthcare system. It is quite challenging to design the intrusion detection and prevention procedure. Hence a security monitoring architecture has been developed through the analysis of the DNS traffic, IP flow records, HTTP traffic, and the honey pot data [33,38], where the solution suggested consists of storing and processing data, in distributed sources through data correlation scheme.

8.4.9 Security model for healthcare in wireless sensor network

The growth of wireless sensor networks is increasing at a rapid pace. Various healthcare devices and applications, for example, monitoring of heart rate, temperature, blood pressure, etc. are based on WSN technology as highlighted in Figure 8.11. As major devices and applications are wireless in nature, the data becomes more susceptible to attacks, for example, if an attacker breaks in WSN network, can tamper with patient's nodes, damage the nodes, and even tamper the personal medical records [39].

The security aspects of wireless sensor network have always been a hot topic of research and discussion and its application in healthcare has recently gained tremendous attention among researchers to propose some novel techniques to improvise healthcare technology.

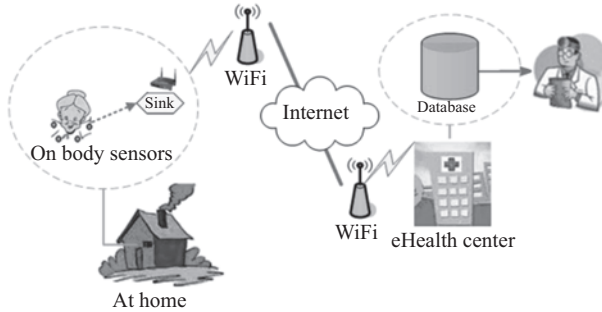


Figure 8.11 WSN based e-healthcare center

The attacks that are susceptible to a healthcare system using WSN are:

- Data modification
- Impersonation attack
- Eavesdropping
- Replaying

These attack types can be either internal or external types hampering the network in a variety of ways [36,40].

Defending the threats and security procedures: To counterfeit and combat major threats, the following two security mechanisms are applied:

- (a) Encryption mechanism
- (b) Authentication mechanism

Encryption—The Encryption mechanism in WSN requires all the data to be in encrypted before transmission over the wireless medium. Various researchers have proposed novel methods to enforce data security in the participating nodes within a healthcare system. Zhu *et al.* [41] proposed a novel secured Id based cryptography architecture to support a secured communication between a multidomain wireless mesh network. This architecture can be stretched beyond into healthcare applications which further proves, clients may enjoy a secured service even at roaming mode. Ma *et al.* [42] claims that previously designed defense models are unsuitable to be implemented for an unattended WSN setting.

Authentication mechanism—The privacy is yet another concern in a WSN environment. The data transmitted by the patients with a wireless mode of communication may prove to be fatal when lacks a proper privacy mechanism. Few researchers have mentioned the necessity of proper privacy mechanism in the WSN highlighting few queries to be addressed while designing such as:

1. Who can view the medical records?
2. Who is authorized to view patient records without his/her consent during emergency?
3. Who is responsible for data maintenance and is considered accountable while problem arises?

8.4.10 HIPAA privacy rules

The Health Insurance Portability and Accountability Act (HIPAA) passed in 1996 as a public law was enacted on August 21, 1999. HIPAA section 201-264, collectively referred as Administrative Simplification Provision, need its standard to be publicized by HSS secretary as specified by Electronic Exchange Privacy and Security for Health Information. The HIPAA privacy rules form the national standard in order to protect the patients' health records that regulate the electronic healthcare transactions. The HIPAA rules require efficient cum safeguarding measures to protect the privacy of personal healthcare information. It also sets limits cum conditions on the utilization as well as disclosure of vital information without consent of the patient. The rule also gives right to the patient's over their health record's information which includes right to examination as well as acquiring a copy of health records, and making corrections, if required [42,43].

The privacy rule and other administrative simplification rules formed in HIPAA are applicable to health plans, healthcare, clearing house as well as healthcare providers that can transfer health information in electronic format.

8.5 Introduction to algorithms for security and privacy of healthcare system

Healthcare IT industry has emerged as one of the key technologies that allows the highest quality of services to the consumers and patients. Many hospitals are adopting healthcare IT solutions to stand ahead of other competing hospitals. However, the healthcare IT is complex and heterogeneous due to the recent advancement in enhanced computing technologies [44–47]. Although, healthcare IT system has several new opportunities for competitive advantages, there are some serious security and privacy concerns need to be addressed. Data Security is addressed as the mechanism through which the data are securely stored and then transferred to the data storage systems. The data storage system may be centralized or distributed. Data privacy refers the authorization of device or people to access the healthcare records stored on remote systems. The major focus of this section is to analyze various algorithms involved in the above three approaches with respect to security and privacy in Healthcare IT [48].

Generally, the huge quantity of healthcare records is stored on remote storage systems such as cloud and dedicated servers. The remotely stored data can be accessed in a distributive manner for further processing. In order to maintain dependability various error correcting codes are used. To maintain level of confidentiality, encryption technique like homomorphism encryption is involved and digital signatures are used to maintain integrity [49].

Next, the objectives of data access security involve threat analysis, access control, data sharing, and accountability. It is equally essential to protect the integrity of medical records from outside threats such as modification, data deletion by intruders via hacking device and network vulnerabilities. Therefore, threat Analysis for Electronic Health records (EHRs) require data tempering detection and

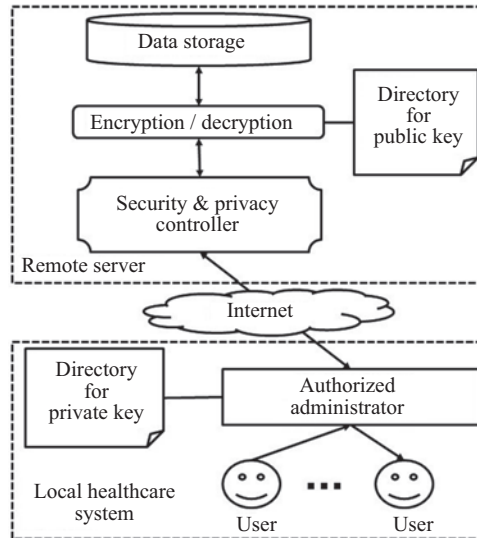


Figure 8.12 Generic cryptography process for healthcare data

data authentication mechanisms. Also, the access control of the sensitive data has to be defined to overcome threats. The access control mechanism involves strict policy framework, role-based access control, and criticality aware access control mechanism. According to literature, the schemes such as secret key cryptography (SKC) and public key cryptography (PKC) are effective mechanisms to maintain security and privacy [33–35]. The data sharing mechanism involves data mining based on encrypted data (DMED). Also, deep learning algorithms are widely popular for preserving privacy of huge healthcare data. Further, in literature, the Map Reduce mechanism is used for accountability [38].

The next level of security and privacy for healthcare data is based on Authentication. The authentication is performed either on human or device. Generally, security principle, that is, two-way authentication is used. Based on which, the patient or consumer authentication is performed using username and password validation, along with dynamically generated one-time key (OTA) sent to the handled devices. On the other hand, the device authentication on constrained handheld healthcare sensors is performed using light weight authentications schemes.

8.6 Data storage security

According to [48] the data storage security is ensured using three performance parameters namely confidentiality, dependability, and integrity.

Confidentiality: Confidentiality prevents the leakage of patient information at the time of storage as well as retrieval from the storage systems. Therefore, it is essential to maintain the confidentiality of critical data, irrespective of the remote

storage system or local storage system. Further, the confidentiality mechanism should not be vulnerable to device compromised attacks. In the sense, the storage devices should not be compromised by any sort of leniency. Rather, the confidentiality mechanisms should prohibit or avoid the intentional attacker to access to the data on the remote or local storage systems.

Dependability: Dependability ensures the correctness of data without any failure encounter at the time of retrieval from remote or local storage systems. Various malicious activities like a Byzantine node failure and data modification makes a serious impact toward dependability. Hence it is essential to provide a security mechanism to overcome such vulnerabilities in patient's data.

Integrity: Integrity ensures unaltered and unmodified critical patient's data. It is evident that the modification of data will lead to disastrous complications during diagnosis of the patients. Hence, the integrity of data should be monitored and protected at all times continuously. The integrity of data should be maintained during storage, retrieval and transmission of critical data across the data storage systems. The system for monitoring the data integrity should be capable of monitoring as well as detect any unauthorized access or altering of data by malicious attackers. In such situation the integrity of the system should warn and also send alerts to the users effectively.

The most popular solution to maintain these parameters are Redundant Residual Number systems (RRNS), Algebraic Signatures, and Catch Me (If You Can) storage mechanisms.

Redundant residual number systems (RRNS): The authors in [49,50] discussed the role of RRNS in the healthcare applications. The principle of RRNS is to incorporate distributed data storage systems. To ensure the security for such a system, RNN involves an integer number-based mechanism. An integer number along with the residues of that integer X are used as a distributed security mechanism. The residues are set of integers " x " representing the moduli of the integer X . Hence the integer is represented as $X + r$, where r represents the redundant moduli. According to RRNS mechanism any file F from the source data systems " S " is distributed among " n " different other data storage systems. Hence, the n nodes are identified using $n=X+ r$ moduli along with residual vectors of file " F ." Based on the residue vector and values of n , the file " F " is distributed at different data storage node. In case of recovering the original file " F ," the node " n " must be authorized by gathering enough and correct residual vector from the other $(n-1)$ storage nodes. It is evident that this mechanism of distributed data storage system ensures the performance factors like dependability, confidentiality, and integrity.

Algebraic signatures: The algebraic signature method was proposed by [51]. The original data are encrypted using cryptographic algorithms. Then, the encrypted data at the source data storage system are shared between n units of data blocks. These " N " units of data blocks are then coded schematically using (N, k) encoding. The algebraic signature of a data block consists of $n_1, n_2, n_3... n_i$ as follows:

$$sign((n_1, n_2, \dots, n_i), k) = \sum_{i=1}^N n_i \cdot k^i \quad (8.1)$$

Similarly, the secret key is shared using (N, k) secret key coding scheme. Once, the data and its corresponding secret key are coded using algebraic signatures of (N, k) , then the “N” data blocks are shared among N distributed data storage systems. In order for any node “ n_i ” request to retrieve the original data from the serving node “S,” then each of these nodes has to compute algebraic signatures using (N, k) coding of its data share and then distribute the computed algebraic signature to the serving node. In turn, the serving node will verify the broadcasted algebraic signatures. Upon the verification, the original data are provided to the requesting node “N” by the serving node “S.” The algebraic property of different algebraic signatures of two data blocks A_i and B_i is verified as follows:

$$\text{sign}(A, k) + \text{sign}(B, k) \quad (8.2)$$

$$= \text{sign}((a_1, a_2, \dots, a_i), k) + \text{sign}((b_1, b_2, \dots, b_i), k) \quad (8.3)$$

$$= \sum_{i=1}^N a_i.k^i + \sum_{i=1}^N b_i.k^i \quad (8.4)$$

$$= \sum_{i=1}^N (a_i + b_i).k^i \quad (8.5)$$

$$= \text{sign}((A + B), k) \quad (8.6)$$

Catch Me (If You Can): Catch Me (If You Can) mechanism was proposed by [52]. In certain situation, the attackers are already aware about the source node of data storage systems. It is obvious that, in such situations, the attackers may target only specific nodes using a pattern of attacks. In order to overcome these types of malicious attacks, it is preferable to handle by importing the sensitivity data to different nodes at a regular time interval. The main purpose of this mechanism is that, it makes the attackers difficult to carry out attacks specific to particular nodes and its stored data information. This mechanism improves the survival probability to larger extend. Further, to enhance the data security on storage system, in addition to this, application data, cryptographic algorithms are incorporated.

8.6.1 Threat analysis

The information system for healthcare is vulnerable to different type of threats. In recent years, such threats have caused huge damage to the healthcare database systems and hence a huge loss in the maintenance of HIS records [37–40].

The threats to HIS can be broadly classified into six categories as described below:

- **Natural threats:** The threats that are not caused by any activity of human kind, but due to the nature of the surroundings. Such threats include natural calamities like earthquake, flood, cyclone, forest fire, etc. The natural threats are dependent on the place and the location of healthcare organization and HIS on the earth. For example, the HIS located in earthquake prone zones, may be affected by the frequent high rector scale of earthquakes. Further, in such

cases, HIS components like hardware, software and support systems might be generally damaged or completely destroyed due to such natural phenomenon.

- **Intentional threats:** The intentional threats are deliberately caused by human. These threats constitute completely wrecking of data, unscrupulous way of handling hardware, software, and healthcare information. These threats are caused by the attackers in the forms of malicious techniques such as malware, spyware, data theft, and fraudulent activities. The factors that alleviate such intentional threats are, the lack of updating of security software, hardware, and physical aspects.
- **Unintentional threats:** Unintentional threats are caused due to omission of required information, semantic, and syntactic errors in software for healthcare IS. These types of errors are mostly human initiated due to negligence or unawareness of the importance of information. Although such actions are not intentional.
- **Transmission threats:** Transmission threats involve the unintentional failure of transmission systems such as link, nodes, router, and switching systems. These types of failure might lead to huge loss of data and hence create a threat to the information. However, the intentional transmission threats involve any attacker might perform tapping of the transmission link by means of unauthentic tapping of information. Particularly in wireless-based transmission, the air medium is open to everybody. In this case, the attackers may interfere or tap the information. Hence, the HIS vulnerable to transmission threats. The major reason for the loss in unintentional transmission threats is due to an insufficient backup of redundant systems.
- **Network threats:** Network system threat involves spoofing of IP address, phishing of information, denial of service attack, malware, virus, worm, and spyware of the network information exchange. The network protocol and operating systems are highly vulnerable to such kind of network threats. The major reason for network threat is due to inefficient firewalls and intrusion detection systems. Further, in [53] authors addressed the effect of heat dissipation in the data center of HIS can lead to critical threats for healthcare information. Solutions to such threats involve, improvisation of the cooling system of data storage systems and availability of redundant distributed data handling centers.
- **Information threats:** Information is highly important, and most of the organizations has realized that information security risks can impact business coherence and trademark, and even associates. Information threats can lead to financial adversity, impact connections with customers and collaborators and their requirements [53]. Thus, security towards information threat provides assurance of data and its crucial components. In recent years, cyber hackers use intensified techniques and mechanisms to attack targets. Instead of developing Internet-based virus, worms, and malware, the attackers are currently focusing on security breach, stealing sensitive information, and data manipulations. Most of the common information security setup is vulnerable to all sorts of threats by outside world and has to be configured significantly by professional

cyber security experts. The intension of cyber hackers is to gather sensitive information from the home users. The prominent techniques for hacking are web program attacks, surfacing, and desktop software applications.

8.7 **Data access security**

- ***Role-based access control (RBAC)***

According to [54] healthcare information is primarily user specific and often professional role dependent as illustrated in Figure 8.13 below. For example, if a patient “A” records need to be accessed by patient “A,” neuro surgeon “B,” and staff in charge “C” with no access to any other persons from other departments. To facilitate this, there is a necessity of fine grained data access control mechanism. Furthermore, the healthcare information system should have context aware-based data access control. And, the data control model must take care of the dynamism in context aware with respect to temporal and space factors.

- ***Criticality aware access control (CAAC)***

In case of medical emergencies, the access control has to be leveraged proactively. The role-based access control model has to follow strict rules for data access, which may not be well suited to the data access during an emergency medical condition scenario [55]. Rather, the data access mechanism should be flexible while accessing data under medical emergencies. However, both these types of data access control mechanism must provide security along with

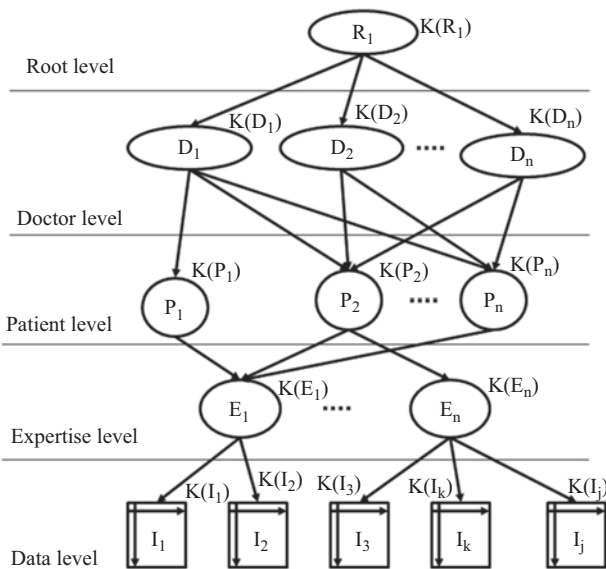


Figure 8.13 Example of role-based access control mechanism

complex and strict data access policies. Also, the security measures are required to avoid any type of malicious attacks on data, compromised storage attacks, and illegitimate user attacks.

To perform security the two basic security mechanisms namely Symmetric Key Cryptography (SKC) and Public Key Cryptography (PKC) are considered highly efficient. The mechanisms are elaborated as follows:

- **Symmetric key cryptography (SKC)**

The authors in [56] discussed the symmetric key cryptography (SKC), the mechanism uses the Blundo's key for providing role-based data access mechanism in healthcare systems. The Blundo's key is predistributed using polynomial-based key and is shared among the legitimate users. Upon grant of access control, the patient or legitimate user can view the necessary healthcare records. The entities used for key establishment are cryptographic-based keying material (CKM), light weighted digital certificate (LDC) that is linked with each KM, and a policy corresponding to each security mechanism. The keying material (KM) is involved in distributing the key establishment agreement using multidimensional α secure key establishment (MaSKE) mechanism. Then, LDC manages and stores the user identify and access control responsibility in digital form. Each entity involved in SKC has to hold individual security policies with respect to its specific role and how to interact with peer entities.

However, some of the disadvantages of SKC-based data access control are that it is difficult to establish the fine-grained data access control because of the complexity involved in key generation and management. Further, the collision of data access due to multiple user requests for the same data is highly possible. Hence, the solution of encrypting only once for the entire security process of data access is most preferable. For this purpose, public key cryptography (PKC) is best suitable.

8.7.1 Public key cryptography

The objective of public key cryptography (PKC) is to provide fine-grained data access control. Unlike SKC method of one to one encryption, the PKC method provides one-to-many encrypted data transactions. The security aspect as the confidentiality, dependability, and integrity are well ensured in PKC. The SKC-based encryption involves more computation cost due to complexity in key generation and management. While, the PKC algorithm reduces the computation cost by outsourcing heavy computation to remote cloud servers [57]. The Attributed Based Encryption (ABE) is an effective technique under public key cryptography. The following section elaborates the ABE scheme in detail.

Attribute-based encryption (ABE): The ABE algorithm was proposed by [55], primarily targets computation cost reduction via outsource mechanism. Accordingly, the ABE incorporates semitrusted remote cloud server to compute the El Gamma-based cipher data for any ABE-based cipher data. Thus, the users are required to perform less computation in order to retrieve the original plain text data. The main advantage of ABE is that the remote semitrusted server need not require

to be known regarding the original plain text as well as the secret key of the users. Instead, the user has to generate two simple keys, namely blind key (BK) and retrieving key (RK). Upon providing the blind key (BK) by the user to the remote cloud server, the later produces the El Gamma-based cipher text as output to the user. Then, the El Gamma based cipher text is converted into the original text at the user side by using the retrieving key (RK). However, the major drawback of this ABE scheme is that, the proof of correctness for the cipher text transformation. The correctness is essential to be verified as it involves the semitrusted remote cloud server. In order to perform verifiability of correctness, the ABE scheme has two methods, namely cipher text policy (CP-ABE) and key policy (KP-ABE).

Ciphertext policy-based ABE (CP-ABE): The CP-ABE scheme is discussed in [58–60]. In this, an access policy mechanism is associated to each cipher text generated under ABE scheme. Further, a Secret Key (SK) is associated with each set of descriptive attributes (DA) that represents individual user. Algorithm 1 depicts various steps involved in CP-ABE algorithm. The major advantage of this method is that, the ABE cipher text can be decrypted only when the access policies are available for each of the encrypted descriptive attributed set. The encryption performs monotonically represented access structure (A) that satisfies the threshold value of descriptive attributes. Thus, CP-ABE is more powerful in terms of verifiability of correctness of the original text. However, the disadvantage of CP-ABE algorithm is the rigid access control which is not suitable for healthcare organizations that require flexible access control, according to different users. This happens due to the factor that CP-ABE algorithm requires a complete structured way of descriptive attributes for each legitimate user to access the system [61].

Algorithm: CP_ABE

Input: access structure = A; secret key= SK ; descriptive attribute= DA;
message= M;

```
Func_Initialize(security parameter) => {PK, MK }
Func_Encryption(PK, M,A)             => { CT }
Func_KeyGeneneration(MK, DA)         => { SK }
Func_Decrypt(CT, SK )                => { M           ; if DAεA
                                           Invalid        ;otherwise }
```

Key policy-based ABE (KP-ABE): To overcome the disadvantages of AES, [62] proposed an efficient scheme called key policy-based ABE (KP-ABE). Basically, in KP-ABE along with cipher text two other components are associated [62,63]. The first component is the set of descriptive attributes (DA) annotated with each user. Next, the secret key (SK) is associated with access policy (A) related to an individual user. The KP-ABE method performs reverse of CP-ABE method. Algorithm 2 depicts the steps involved in KP-ABE method. In this, the cipher text

(CT) of the message (M) is generated based on the DA, and the secret key is generated using access policy (A). This way the KP-ABE scheme performs verification for correctness of the cipher text transformation from El Gamma-based on ABE cipher text and vice versa.

Algorithm: KP_ABE

Input: access structure = A; secret key= SK ; descriptive attribute= DA;
message= M;

```

Func_Initialize(security parameter) => {PK, MK }
Func_Encryption(PK, M, DA^A)      => { CT }
Func_KeyGeneration(MK, A)         => { SK }
Func_Decrypt(CT, SK )              => { M           ; if DA ∈ A
                                   { Invalid        ; otherwise

```

Hybridized CP and KP-based ABE (CP-KEM-ABE): In addition to CP-ABE and KEM-ABE, [62] proposed hybridization of the CP and KEM along with ABE scheme, known as cipher text policy attributed based key encapsulation mechanism (CP-KEM-ABE). This hybridization mechanism ensures the verifiability of outsourced cipher texting. The major advantage of this scheme is that users are not vulnerable to the incorrectness of the results of the encryption and decryption process and computation outsourcing to semitrusted remote cloud servers [63].

Algorithm: ABS

Input: access structure = A; secret key= SK ; descriptive attribute= DA;
message= M;

```

Func_Initialize(General security parameter) => {TPK }
Func_Initialize(Attribute based security parameter) => {APK, ASK }
Func_Attr(ASK, A)                               => { SK }
Func_Signature(PK=(TPK,APK),SK,M,ψ)              => γ
Func_Validation(PK,M,ψ,γ )                        => Boolean Value

```

Accountability

Attribute-based signatures (ABS): The author in [64,65] introduced the attributed based signatures (ABS). Under ABS scheme, in addition to the basic ABE security scheme, some enhanced features are also included such as, the end-user includes digital signatures as well as the set of attributes for further encryption to be carried out. The major objectives of ABS scheme are to ensure the type of signature and

Table 8.1 *Types of signature schemes*

Signature schemes	Message endorsement
Group signatures	List of possible signers
Ring signatures	Public, ad hoc signer
Mesh signatures	Signer with standard signatures
Attribute-based signatures (ABS)	Set of signer attributes

also the accountability of the user who signed the specific transaction. Further, a user accountability is ensured through bilinear pairing approach over monotone group of users. The ABE scheme requires an intensive semantics in order to handle the profound anonymity. The other types of digital signatures such as group, mesh and ring signatures target only signer anonymity and undeceitful as depicted in Table 8.1 below. While, the ABS scheme provides a description of a user message along with the predicated set of attributes. The basic objective of ABS is that the colluding parties should not be able to create collude key pool by combining their attributes [66].

The main advantages of these two schemes are that they support limited forms of digital signatures. And also, the length of these digital signatures expands linearly in proportional to the attributes associated with the individual users. Alternatively, nonmonotone ABS-based digital signature was discussed by [61]. The nonmonotonic scheme incorporates multiple authorities for handling digital signatures. Moreover, the signatures are constant in size and supports large number of attributes associated with each user.

The parameters used for attribute-based signature (ABS) are A , the set of attributes. The claim predicate (Ψ) of attributes belong to A are monotone function with Boolean output. The ABS has four subfunctions as shown in algorithm below.

8.7.2 *Data sharing security*

In recent years an enormous amount of data is generated through healthcare information systems, electronic health records, patient health records, medial medical images, hospital management systems, and clinical information systems. To handle such voluminous data, cloud computing and big data technologies are widely used. The added advantages of cloud computing is that computing resources and storage facility can be obtained as a service on demand from the remote cloud servers which is charged based on usage basis. However, the major challenge in such information sharing platform is trust, security, and privacy issues. Several schemes are proposed in literature for providing security in data sharing environment [49,55]. The most popular schemes are Accountable Map reduce, Semantically Secured Encrypted Relational Data, Data Mining over encrypted data (DMED), Privacy Preserving K-NN, Attribute Based Encryption, Sticky Policy Framework, and Homomorphism Encryption.

8.8 Authentication

- **Image data authentication**

The healthcare platform involves lots of images as input data. These images are transmitted on remote server or health systems of customers. During the image data transmission, the actual image gets tampered either intentionally by malicious attackers or unintentionally by users. These types of tampering in the original images adversely affect the diagnostic process of patients. In order to circumvent the unauthenticated usage or causing damage to the authenticity of the image data, the image authentication mechanisms are used. The image authentication involves two major techniques, namely digital watermarking and stenography.

- **Digital watermarking**

In digital watermarking technology, the authentication information is deliberately embedded within normal image data. Upon the transmission of digitally watermarked image data, the receiver of the secured data will extract the embedded authentication information and then compared with the negotiated watermarks, so as to the reliability of the transmitted image data is ensured. The embedding process of digital watermarking is performed at frequency domain and space domain.

- **Frequency domain**

The frequency domain-based image authentication involves two major methods, namely discrete cosine transformation (DCT) and discrete Fourier Transformation (DFT).

- **Discrete cosine transformation**

The first step in discrete cosine transformation (DCT) is to estimate the undetermined coefficients based on the input image data. Then, the second step involves replacing the undetermined coefficient with preferable information for authentication. The third step is to apply DCT on the resultant image. The formula for DCT is given by

$$G(x, y) = \frac{2}{M} \sum_{u=0}^{M-1} \sum_{v=0}^{M-1} g(u, v) \cos \left[\frac{(2u+1)x\pi}{2M} \right] \cos \left[\frac{(2v+1)y\pi}{2M} \right] \quad (8.7)$$

- **Discrete Fourier transformation**

The first step of discrete Fourier transformation (DFT) is to convert the image from the spatial domain into its respective frequency domain using the DFT formula given by the equation given below.

$$G(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{M-1} g(u, v) e^{-j2\pi(xuN + yvM)} \quad (8.8)$$

The second step of the DFT watermarking involves embedding of image authentication information at the upper level frequency and the middle level frequency elements. In order to fetch the decrypted image, the inverse of the DFT function is performed at the receiver side.

- ***Spatial domain-based digital image embedding***

Spatial domain involves the estimation of least significant bit (LSB). The main advantage of LSB method is that, the image quality will not be affected. The LSB method works on the principle of one-bit error checking code. The 7th bit as Most Significant Bit (MSB) is then coupled along with the one-bit LSB error checking code. This mechanism is then used to inspect any tampering of original medical image data. The major advantage of the spatial domain-based image authentication mechanism is due to its simple procedure yet effective in terms of providing image authentication.

- ***Stenography***

The process of stenography involves hiding of the original message that is exchanged between the source and destination. Figure 8.14 illustrates the process of stenography. The binary data of the source message is contained within the original image. In order to protect the message, the message is encoded by the stenographic key. Then, each pixel of the original image will carry the encoded message. The modified image, thus called as stenographic image, carry the encrypted message. In the field of imaging-based healthcare information system, the owner rights are protected and also the privacy of the patient is maintained. Medical images are generated through different source of image scan mechanisms like Mammography, positron emission tomography (PET), computed axial tomography (CT scan), and magnetic resonance imaging (MRI) [67,68].

These medical imaging scanning systems produce large number of image-based data. The image data need to be associated with several important about

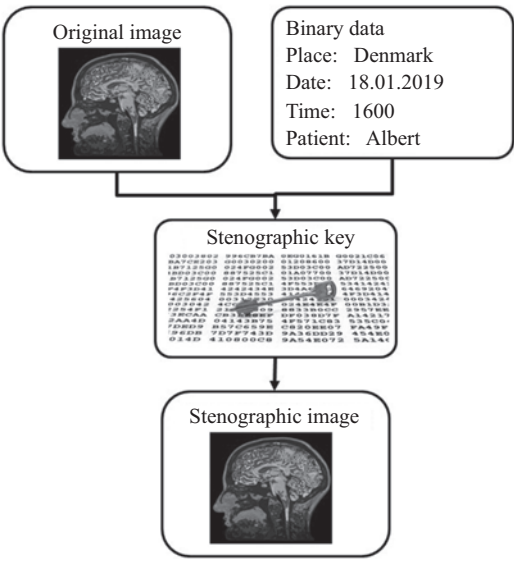


Figure 8.14 Basic flow of stenographic technique

patient and image information. For example, the details of the medical image may include patient name, identity of image, source of the image (PET, MRI, or CT scans), health center name, and date of the image taken. The image information is converted into binary data and embedded into the pixels of medical image using cryptographic techniques. Further, the upper left corner of the image will be watermarked using Unicode. For extracting the original information and image, the reverse process is performed. The information is extracted from the binary value of the image and then extracted bits are converted into ASCII code of characters to retrieve the original text of image information.

- **Device authentication**

The smart healthcare hardware devices provide critical information regarding patients and the environment. It is essential to assure device security, and authenticity of users via device authentication mechanisms. However, these devices are mostly resource constrained in terms of computing capability, energy utilization, memory capacity, and network QoS. Hence, the design goal for any authentication mechanism for healthcare devices involves legitimate authentication of medical devices connected via remote systems or local controlling units. Further, it requires strong key generation and management policies, and finally the authentication system must be resilient to all sorts of security threats and attacks coming from the outside world. The authors in [67] proposed binding protocol for public medical devices to perform live streaming of data via wireless/wired transmission to remote servers in a secure way. In case of wireless body area network (WBAN) [69,70], these devices are particularly vulnerable to impersonation attacks. A solution to this problem was proposed by [68] via Anonymous Authentication Scheme for impersonation attacks. Next, [55,71] proposed light weight authentication mechanism that handles the interconnection of medical sensor nodes with the remote user. In this, Exclusive OR and Keyed Hash message authentication is used to verify the integrity of each transaction between the devices, user, and controlling systems of the devices. XOR manipulation methods are used for encryption [72].

8.9 Conclusion

Healthcare is a vital aspect of the society where, accidents and emergencies constantly pose a threat to human life-giving birth to need of hospitals, which can diagnose, treat, and manage different types of ailment or disease. With uplift of technology and growth of digitization all over the world, our healthcare organizations have also incorporated the electronic mode of work management, introducing the concept of EHR which is though beneficial is not free from attacks. It is very important to apt the e-health care system with effective security and privacy measures.

The chapter primarily concentrates over the Security aspects of a Healthcare organization. It discusses on the various current security models and measures adopted and its suitability to a healthcare sector. Further, it presents various proposed models by various researchers which may be further worked upon and

adopted into practice. The chapter discusses the various algorithms that have been implemented as well as proposed as a measure to enforce both privacy and security aspects of the healthcare.

With the growth of various recent security mechanisms that can all the more strengthen the overgrowing technology, be it communication or storing databases like big data, cloud data, etc., all can be incorporated in a healthcare organization immensely benefiting both the hospitals as well as human life.

8.10 Future scope

Future of the research would aim at implementing healthcare services in recent technology like ad hoc network, mobile phones or smartphone-based e-healthcare, wireless body sensor network (WBSN) based e-healthcare systems, tele-home patient monitoring, system-on-chip e-healthcare modules, and towards designing and testing more secured and adaptive strategies which include Swarm Intelligent or machine learning based techniques like ACO, PSO, etc. for further improving the performance of security algorithm in terms of reliability, security, fault tolerance, and availability.

References

- [1] Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., & Russell, J. (2010). Adoption, non adoption, and abandonment of a personal electronic health record. *A Case Study of Health Space* [Accessed January 20, 2019].
- [2] Allard, T., Anciaux, N., Bouganim, L., *et al.* (2010). Secure personal data servers: a vision paper. *Proceedings of the VLDB Endowment*, 3(1–2), 25–35.
- [3] Nayyar, A., Puri, V., & Nguyen, N. G. (2019). BioSenHealth 1.0: a novel Internet of medical things (IoMT)-based patient health monitoring system. In *International Conference on Innovative Computing and Communications* (pp. 155–164). Springer, Singapore.
- [4] Batth, R. S., Nayyar, A., & Nagpal, A. Internet of robotic things: driving intelligent robotics of future-concept, architecture, applications and technologies. In *2018 4th International Conference on Computing Sciences (ICCS)* (pp. 151–160). Jalandhar: IEEE.
- [5] Nayyar, A., Ba, C. H., Duc, N. P. C., & Binh, H. D. (2018, August). Smart-IoUT 1.0: a smart aquatic monitoring network based on Internet of underwater things (IoUT). In *International Conference on Industrial Networks and Intelligent Systems* (pp. 191–207). Springer, Cham.
- [6] Nayyar, A., Mahapatra, B., Le, D., & Suseendran, G. (2018). Virtual reality (VR) and augmented reality (AR) technologies for tourism and hospitality industry. *International Journal of Engineering & Technology*, 7(2.21), 156–160.
- [7] Nayyar, A., Puri, V., Nguyen, N. G., & Le, D. N. (2018). Smart surveillance robot for real-time monitoring and control system in environment and

- industrial applications. In *Information Systems Design and Intelligent Applications* (pp. 229–243). Springer, Singapore.
- [8] Nayyar, A., Puri, V., & Le, D. N. (2017). Internet of nano things (IoNT): next evolutionary step in nanotechnology. *Nanoscience and Nanotechnology*, 7(1), 4–8.
- [9] Anand Nayyar, E., & Puri, V. (2016). “In smart farming: IoT based smart sensors agriculture stick for live temperature and moisture monitoring using Arduino, cloud computing & solar technology” [Online], *The International Conference on Communication and Computing Systems (ICCCS-2016)*. Gurgaon: Springer.
- [10] Kaneriya, S., Tanwar, S., Nayyar, A., *et al.* (2018). Data consumption-aware load forecasting scheme for smart grid systems. In *2018 IEEE Globecom Workshops (GC Wkshps)* (pp. 1–6). Abu Dhabi, United Arab Emirates: IEEE.
- [11] Sainz de Abajo, B., de la Torre Díez, I., Bermejo González, P., *et al.* (2010). Evolución, beneficios y obstáculos en la instantación del Historial Clínico Electrónico en el sistema sanitario. *RevistaeSalud. com*, 6(22).
- [12] Hesse, B. W., Hansen, D., Finholt, T., Munson, S., Kellogg, W., & Thomas, J.C. (2010). Social participation in health 2.0. *Computer*, 43(11), 45–52.
- [13] Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: ensuring privacy of electronic medical records. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security* (pp. 103–114). New York, NY: ACM.
- [14] Los países europeos compartirán las historias clínicas de sus pacientes antes de, 2015. <http://www.europapress.es> [Accessed January 7, 2019].
- [15] Rothstein, M. A. (2007). Health privacy in the electronic age. *The Journal of Legal Medicine*, 28(4), 487–501.
- [16] Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: lessons learned from a comparative study. *Journal of Medical Systems*, 34(4), 629–642.
- [17] Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International Journal of Medical Informatics*, 80(2), e26–e31.
- [18] Aginam, O. (2005). Bio-terrorism, human security and public health: can international law bring them together in an age of globalization. *Medicine and Law*, 24, 455.
- [19] Pibulsonggram, N., Amorim, C., Douste-Blazy, P., Wirayuda, H., Støre, J. G., & Gadio, C. T. (2007). Oslo Ministerial Declaration–global health: a pressing foreign policy issue of our time. *Lancet*, 369(9570), 1373–1378.
- [20] Axworthy, L. (2001). Human security and global governance: putting people first. *Global governance*, 7, 19.
- [21] Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, 23(1), 5–26.
- [22] Bristol, N. (2006). Military incursions into aid work anger humanitarian groups. *The Lancet*, 367(9508), 384–386.

- [23] Calain, P. (2007). Exploring the international arena of global public health surveillance. *Health Policy and Planning*, 22(1), 2–12.
- [24] Calain, P. (2007). From the field side of the binoculars: a different view on global public health surveillance. *Health Policy and Planning*, 22(1), 13–20.
- [25] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2), 38–47.
- [26] Sandhu, R., Bhamidipati, V., Coyne, E., Ganta, S., & Youman, C. (1997). The ARBAC97 model for role-based administration of roles: preliminary description and outline. In *Proceedings of the Second ACM Workshop on Role-Based Access Control* (pp. 41–50). New York, NY: ACM.
- [27] Ferraiolo, D., Cugini, J., & Kuhn, D. R. (1995). Role-based access control (RBAC): Features and motivations. In *Proceedings of 11th Annual Computer Security Application Conference* (pp. 241–48). New York, NY: ACM.
- [28] Peiying Shao & Shuling Su. (1999). Security design and implementation based on traditional mandatory access control. *Computer Engineering and Applications*, 8, 58–60.
- [29] Singh, S. P., Nayyar, A., Kaur, H., & Singla, A. (2019). Dynamic task scheduling using balanced VM allocation policy for fog computing platforms. *Scalable Computing: Practice and Experience*, 20(2), 433–456.
- [30] Kaur, A., Gupta, P., Singh, M., & Nayyar, A. (2019). Data placement in era of cloud computing: a survey, taxonomy and open research issues. *Scalable Computing: Practice and Experience*, 20(2), 377–398.
- [31] Singh, P., Gupta, P., Jyoti, K., & Nayyar, A. (2019). Research on auto-scaling of web applications in cloud: survey, trends and future directions. *Scalable Computing: Practice and Experience*, 20(2), 399–432.
- [32] Nayyar, A. (2011). Interoperability of cloud computing with web services. *International Journal of ElectroComputational World & Knowledge Interface*, 1(1).
- [33] Marlin. (2006). Marlin architecture overview. *Marlin Developer Community*. Available Online at <https://www.marlin-community.com/public/MarlinArchitectureOverview.pdf> [Accessed January 21, 2019]
- [34] Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics*, 18(4), 1431–1441.
- [35] AbuKhoua, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-health cloud: opportunities and challenges. *Future Internet*, 4(3), 621–645.
- [36] Benson, T. (2010). *Principles of Health Interoperability HL7 and SNOMED* (p. 263). London: Springer.
- [37] Birnhack, M. D. (2008). The EU Data Protection Directive: an engine of a global regime. *Computer Law & Security Review*, 24(6), 508–520 [Accessed January 20, 2019].
- [38] Brailer, D. J. (2005). Interoperability: the key to the future health care system: Interoperability will bind together a wide network of real-time, life-

- critical data that not only transform but become health care. *Health Affairs*, 24(Suppl 1), W5–W19.
- [39] Campbell, A. T., Eisenman, S. B., Lane, N. D., *et al.* (2008). The rise of people-centric sensing. *IEEE Internet Computing*, 12(4).
 - [40] Dohler, M. (2008). Wireless sensor networks: the biggest cross-community design exercise to-date. *Recent Patents on Computer Science*, 1(1), 9–25.
 - [41] Zhu, X., Fang, Y., & Wang, Y. (2010). How to secure multi-domain wireless mesh networks. *Wireless Networks*, 16(5), 1215–1222.
 - [42] Ma, D., Soriente, C., & Tsudik, G. (2009). New adversary and new threats: security in unattended sensor networks. *IEEE Network*, 23(2), 43–48.
 - [43] Kargl, F., Lawrence, E., Fischer, M., & Lim, Y. Y. (2008). Security, privacy and legal issues in pervasive ehealth monitoring systems. In *7th International Conference on Mobile Business, 2008. ICMB'08.* (pp. 296–304). Washington, DC: IEEE Computer Society.
 - [44] Solanki, A., & Nayyar, A. (2019). Green Internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In *Handbook of Research on Big Data and the IoT* (pp. 379–405). Hershey, PA: IGI Global.
 - [45] Singh, S. P., Nayyar, A., Kumar, R., & Sharma, A. (2018). Fog computing: from architecture to edge computing and big data processing. *The Journal of Supercomputing*, 75(4), 2070–2105.
 - [46] Nayyar, A., Jain, R., Mahapatra, B., & Singh, A. (2019). Cyber security challenges for smart cities. In *Driving the Development, Management, and Sustainability of Cognitive Cities* (pp. 27–54). Hershey, PA: IGI Global.
 - [47] Das, S., & Nayyar, A. (2019). Innovative ideas to manage urban traffic congestion in cognitive cities. In *Driving the Development, Management, and Sustainability of Cognitive Cities* (pp. 139–162). Hershey, PA: IGI Global.
 - [48] Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1).
 - [49] Chessa, S., & Maestrini, P. (2003). Dependable and secure data storage and retrieval in mobile, wireless networks. In *Proceedings of the 2003 International Conference on Dependable Systems and Networks, 2003* (p. 207). Rio de Janeiro: IEEE.
 - [50] Chervyakov, N. I., Molahosseini, A. S., Lyakhov, P. A., Babenko, M. G., & Deryabin, M. A. (2017). Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem. *International Journal of Computer Mathematics*, 94(9), 1833–1849.
 - [51] Wang, Q., Ren, K., Yu, S., & Lou, W. (2011). Dependable and secure sensor data storage with dynamic integrity assurance. *ACM Transactions on Sensor Networks (TOSN)*, 8(1), 9.
 - [52] Di Pietro, R., Mancini, L. V., Soriente, C., Spognardi, A., & Tsudik, G. (2008). Catch me (if you can): Data survival in unattended sensor networks. In *Sixth Annual IEEE International Conference on Pervasive Computing*

- and Communications, 2008. PerCom 2008* (pp. 185–194). Hong Kong, China: IEEE.
- [53] Alam, M., Emmanuel, N., Khan, T., Xiang, Y., & Hassan, H. (2018). Garbled role-based access control in the cloud. *Journal of Ambient Intelligence and Humanized Computing*, 9(4), 1153–1166.
- [54] Hosseinpour, F., Siddiqui, A. S., Plosila, J., & Tenhunen, H. (2017, October). A security framework for fog networks based on role-based access control and trust models. In *International Conference on Research and Practical Issues of Enterprise Information Systems* (pp. 168–180). Springer, Cham.
- [55] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89–98). New York, NY: ACM.
- [56] Kocabas, O., Soyata, T., & Aktas, M. K. (2016). Emerging security mechanisms for medical cyber physical systems. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 13(3), 401–416.
- [57] Nikolaenko, V., Weinsberg, U., Ioannidis, S., Joye, M., Boneh, D., & Taft, N. (2013). Privacy-preserving ridge regression on hundreds of millions of records. In *2013 IEEE Symposium on Security and Privacy (SP)* (pp. 334–348). Berkeley, CA: IEEE.
- [58] Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *2007 SP'07 IEEE Symposium on Security and Privacy* (pp. 321–334). Berkeley, CA: IEEE.
- [59] Li, L., Gu, T., Chang, L., Xu, Z., Liu, Y., & Qian, J. (2017). A ciphertext-policy attribute-based encryption based on an ordered binary decision diagram. *IEEE Access*, 5, 1137–1145.
- [60] Lin, G., Hong, H., & Sun, Z. (2017). A collaborative key management protocol in ciphertext policy attribute-based encryption for cloud data sharing. *IEEE Access*, 5, 9464–9475.
- [61] Liu, Z., Liu, Y., & Fan, Y. (2018). Searchable attribute-based signcryption scheme for electronic personal health record. *IEEE Access*, 6, 76381–76394.
- [62] Attrapadung, N., Libert, B., & De Panafieu, E. (2011). Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *International Workshop on Public Key Cryptography* (pp. 90–108). Springer, Berlin, Heidelberg.
- [63] Yu, S., Ren, K., Lou, W., & Li, J. (2009). Defending against key abuse attacks in KP-ABE enabled broadcast systems. In *International Conference on Security and Privacy in Communication Systems* (pp. 311–329). Springer, Berlin, Heidelberg.
- [64] Bhattasali, T., Chaki, R., Chaki, N., & Saeed, K. (2018). An adaptation of context and trust aware workflow oriented access control for remote healthcare. *International Journal of Software Engineering and Knowledge Engineering*, 28(06), 781–810.

- [65] Okamoto, T., & Takashima, K. (2014). Efficient attribute-based signatures for non-monotone predicates in the standard model. *IEEE Transactions on Cloud Computing*, 2(4), 409–421.
- [66] Chen, X., Li, J., Huang, X., Li, J., Xiang, Y., & Wong, D. S. (2014). Secure outsourced attribute-based signatures. *IEEE Transactions on Parallel and Distributed Systems*, 25(12), 3285–3294.
- [67] Kester, Q. A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynor, N. N. (2015). A cryptographic technique for security of medical images in health information systems. *Procedia Computer Science*, 58, 538–543.
- [68] Lee, B. M. (2015). Dynamic data binding protocol between IoT medical device and IoT medical service for mobile healthcare. *International Journal of Smart Home*, 9(6), 141–150.
- [69] Pramanik, P. K. D., Pareek, G., & Nayyar, A. (2019). Security and privacy in remote healthcare: issues, solutions, and standards. In *Telemedicine Technologies* (pp. 201–225). Cambridge, MA: Academic Press.
- [70] Pramanik, P. K. D., Nayyar, A., & Pareek, G. (2019). WBAN: driving e-healthcare beyond telemedicine to remote health monitoring: architecture and protocols. In *Telemedicine Technologies* (pp. 89–119). Cambridge, MA: Academic Press.
- [71] He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2017). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal*, 11(4), 2590–2601.
- [72] Khemissa, H., & Tandjaoui, D. (2016). A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things. In *Wireless Telecommunications Symposium (WTS), 2016* (pp. 1–6). London: IEEE.
- [73] Venkatasubramanian, K., & Gupta, S. K. (2007). Security solutions for pervasive healthcare. *Security in Distributed, Grid, Mobile, and Pervasive Computing*, 349, 1–6.
- [74] Zhang, R., Liu, L., & Xue, R. (2014). Role-based and time-bound access and management of EHR data. *Security and Communication Networks*, 7(6), 994–1015.

This page intentionally left blank

Chapter 9

Information security and privacy in healthcare records: threat analysis, classification, and solutions

*Arjun Khera¹, Dharmesh Singh¹, and
Deepak Kumar Sharma¹*

Information security and privacy in healthcare information system is a very critical matter. The increasing acceptance of information systems by various healthcare institutions and increasing security and privacy concerns among patients, all point to the need for proper frameworks of information security and privacy in place. In this paper, we have analyzed numerous categories of threats to a health information system and have identified threats that are unique to a health information system. Later, we have explored various models and algorithms that may be utilized to alleviate these threats. Finally, we have proposed future directions that may encourage further research into this field.

9.1 Introduction

Healthcare is one of the most data-intensive sector. However, unlike other sectors it has yet not utilized information technology to its full extent for reasons that will be explained later. Electronic health records (EHR) has many benefits. Firstly, traditional paper records are very messy to create, store, and share. Other downsides of using paper records include negative effect on environment, illegible writing, difficulty in managing access control, etc. Secondly, it increases quality of service provided to the patient by (i) reducing storing and retrieving time of patient data, (ii) reducing duplication and increasing consistency, and (iii) providing latest data anytime and anywhere. The data retrieval time becomes especially important in emergency cases where speedy access might save lives. Thirdly, as indicated from other benefits, it increases productivity and efficiency. Financially, Hillestad *et al.* have suggested that US government alone could save \$81 billion USD annually by moving to a Global Healthcare Record system [1].

¹Department of Information Technology, Netaji Subhas University of Technology (formerly Netaji Subhas Institute of Technology), Delhi, India

Although EHR comes with these many advantages, there are few roadblocks that need to be handled before healthcare could reap its benefits. As already mentioned, healthcare management is data-intensive and thus, most of the problems are associated with the data under consideration. An example below will illustrate what may happen when a patient meets a physician.

Bob has been suffering from stomach aches for some time. He decides to visit his physician. Upon discussing his symptoms and going through a physical exam, the physician suspects indigestion and gives Bob some medicine. After few days of still going through the same stomach ache, the physician recommends some blood tests to be performed to know the root cause of your stomach ache. Not long, Bob receives the blood tests which suggest that Bob is in the initial stages of a stomach flu. The physician gives him some antibiotics and, in a week, or so, Bob returns to his normal health.

At each step of this procedure, a lot of data are retrieved or created. For instance, when Bob first meets the physician, the physician needs to assess the medical history of Bob. Also, when the physician recommends him blood tests or antibiotics, new entries are made in his medical history. In a typical case, various tests are conducted before physicians are able to diagnose the problem. Thus, it results into vast amount of data being generated. Not only is it in vast quantities but also it is very complex and difficult to structure. This is because, in healthcare, data are encountered in many different forms. It can range from textual data such as the prescription or the blood report to complex imagery such as X-rays and CT-scan. Apart from the data being of different type, it is very difficult to design a one-for-all data structure approach which hinders useful analysis of data.

The last but the biggest roadblock to fully incorporating information systems in healthcare is the security and privacy concerns regarding healthcare data. Healthcare data is very sensitive to an individual. Physician–patient privilege is one of the core concepts of their relationship. Patients are required to share every information with their physician so that they can be correctly diagnosed and treated. They are especially hesitant to share information in cases related to mental disorders or HIV. It is because of this hesitation that physicians are in a legal obligation in not disclosing any of the information related to their patients. Inappropriate disclosure of this information may lead to various unfavorable consequences such as social stigma, discrimination, etc., not to mention financial losses due to identity theft [2,3]. With so many data breaches occurring every year, consumers are becoming very skeptical about whether the benefits of health information systems outweigh the security and privacy risk they pose [4,5]. Different regulations are in place throughout the world such as HIPAA (in the United States) that try to alleviate these security and privacy concerns.

A lot of research has been put to develop models and algorithms for privacy and security in healthcare information systems (HISs) for many years. The aim of this book chapter is to provide a readable summary of the same and familiarize the readers with some models and algorithms that can be used to provide better security and privacy in HISs. The following is divided into four sections. We will begin

with analysis and classification of threats to information security and privacy. Afterward, we will look at major themes of information security and privacy and healthcare-specific problems that need to be resolved to protect information security and privacy. Later, we will look at different algorithms and models for the above themes that can be implemented. Lastly, we will look at future possibilities and further challenges down the road.

9.2 Threats to information security and privacy

Threats to information security and privacy can be defined as anything that has the potential to compromise information security and privacy. HIPAA recommends three types of safeguards against such threats, that is, *administrative safeguards*, *physical safeguards*, and *technical safeguards*. Since administrative and physical safeguards deal with less technical and more direct threats like unauthorized access by physical intrusion, we will be mainly concerning ourselves with technical safeguards in this paper.

9.2.1 Understanding information security and privacy

Information security, in simple terms, refers to techniques that protect data. The three pillars of information security are confidentiality, integrity, and availability. *Confidentiality* refers to protect disclosure of data to unauthorized entities. *Integrity* means that the data stored are always accurate and reliable. *Availability* means that data are available when required and the system is functional under failures and attacks.

Privacy, on the other hand, is a term that applies to individuals. The exact definition of privacy depends on the beliefs of an individual or a group in context, but it does share some common themes. Privacy generally refers to the right of an individual or a group to control his or her data and to specify how the data are collected, used, and shared. Although information security and privacy do share some common concepts like *confidentiality*, there is a difference between privacy and information security that becomes very significant when the data under consideration is highly sensitive with respect to the individual.

9.2.2 Classification of threats

Before, discussing models and algorithms that reduce these threats, it is important to first classify and understand different types of threats. Threats to information security and privacy can be classified into many different categories based on several different factors. There has been large amount of research in this field and yet very little attention has been brought to systematic classification of threats (especially in health information systems). Mouna Jouini *et al.* have presented a multidimensional approach toward quantitative classification of security threats based on several different factors [6]. This perhaps is one of the most exhaustive

threat classification models which branches into 84 different categories of threats based on source (internal or external), agents (human, environmental or technological), motivation (malicious or nonmalicious), intent (intentional or unintentional), and impact (destruction, disclosure of information, denial of service, etc.). However, a more simplistic and qualitative approach of classifying information security and privacy threats specifically concerning healthcare information has been proposed in [7]. It classifies these threats into two broad categories:

- *Organizational threats*: These types of threats stem from internal agents misusing their privileges or external agents utilizing a vulnerability in the information system to access information of a patient.
- *Systemic threats*: These types of threats are more subtle to describe as they stem from agents abusing the implicit design of information flow in a system to extract information.

9.2.2.1 Organizational threats

These types of threats can acquire forms from a whole spectrum of threats ranging from *just a curious employee misusing their privileges* to *external agents accessing data by forced entry*. This whole range of threats could be differentiated on the basis of four parameters: motives, resources, accessibility, and technical expertise. The level of risk that a threat poses on the organization depends on these four parameters. However, research suggests that organizational threats could be broadly classified into five categories depending upon the complexity of the threat and the risks associated with them.

- *Accidental disclosure*: As the name suggests, threats of this category are accidental in nature. For instance, a patient may send her details via email to a wrong address. Although these threats are not premeditated, these threats pose sufficient amount of risks to the organization that must not be ignored.
- *Insider curiosity*: As the name suggests, these types of threats are normally posed by internal agents. These types of threats are the most difficult to prevent against since internal agents misuse their authorizations for personal use. For instance, a doctor may lookup details about a patient that she has a crush on.
- *Data breach by insider*: Although these types of threats are also posed by internal agents, they are executed with entirely different sets of motives because of which the risks associated with threats in this category are very significant. For instance, an employee may misuse her privilege to send sensitive information to competitors (corporate espionage).
- *Unauthorized access by outsider via physical intrusion*: As the name suggests, these types of threats occur due to physical intrusion. For instance, a robber might gain forced entry to a bank to get credit card information.
- *Unauthorized access by outsider via network system intrusion*: These types of threats involve an outsider gaining access to data by abusing security vulnerabilities in the system. These types of threats can cause great damage to the organization ranging from extracting information (passive attack) or damaging the whole information system (active attack).

9.2.2.2 Systemic threats

These types of threats are usually induced by internal agents who exploit the information flow of the system. In other words, internal agents are able to extract unintended information from data that they are legally authorized to obtain. For instance, when patients disclose their information for medical research purposes, organizations that are part of the information flow may be able to extract patient identification information from that data.

9.3 Information security and privacy disciplines

Nowadays, technology is used in most of the industries to accelerate growth and create new opportunities. There are very little industries that are not affected by this technological revolution. This revolution has been made possible by the advent of the Internet. As of now, there are more than 25 billion devices connected to the Internet and this number is just going to increase. It is estimated that by 2025 around 75 billion devices will become a part of Internet of things (IOT) [8]. As more and more devices are becoming part of this huge network of networks, every device in theory is remotely connected with one another. In other words, theoretically any device is accessible if right amount of expertise is utilized. This poses a huge security risk as no matter what the organization, information security is extremely vital for their continuous operation. Therefore, Information security and privacy has become one of the major focus of the scientific community. Vast amount of research has been devoted into different disciplines or objectives of information security. These disciplines can be broadly categorized into 13 themes and numerous subthemes [9]. We need to concern ourselves with the following themes (or subthemes) in information security and privacy:

- Information access control
- Statistical disclosure control

As shown in Figure 9.1, information access control can alleviate the risk associated with threats that fall in shown categories. Similarly, techniques relating to statistical disclosure control can alleviate risks posed by threats that fall under systemic threats. It should be noted that there are many other themes in information security and privacy but the mentioned themes are most relevant for a HIS.

9.3.1 Information access control

Access control refers to control mechanisms that only allow certain entities to access or modify information of a system based on predetermined policies. Access control has been one of the most researched field since the inception of information security as a separate discipline. And although a health information system has many similar requirements from access control as any other system, there are certain requirements that not only make an information access control mechanism difficult to implement but also proves to be one of the major sources of threats to it.

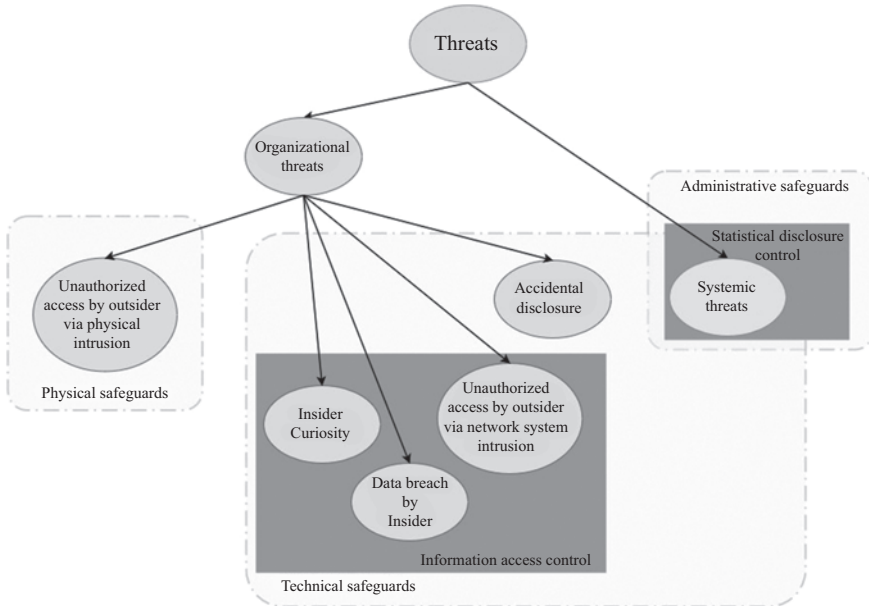


Figure 9.1 Classification of threats with information security themes and HIPAA safeguards

A typical modern health information system is a large networked system managing data of large number of patients with a myriad of users accessing the data for diverse purposes belonging to multiple organizations. A typical hospital may contain more than 20 departments in a single branch not to mention different branches globally. Every department is composed of many different doctors, nurses, etc. and provides/retrieves healthcare data that may not only relate to different aspects of human anatomy but may as well be in different digital formats such as X-ray, CT scan, blood-test reports, etc. Moreover, since many doctors or physicians may belong to many departments simultaneously, hospitals have very complex hierarchical structure. Furthermore, a doctor may consult many peers before reaching a conclusion which further blurs the well-defined boundary of a general information system.

A health information system may be categorized as a *security-critical system* due to the degree of sensitivity of the information it holds. But unlike other security-critical systems such as air traffic control systems, nuclear plant control systems, or online banking systems whose primary goal is information security and privacy, a health information system's primary goal is to provide best service possible to the patient. Therefore, while "when in doubt, deny" may be a general rule in other security-critical systems, a health information system follows "when in doubt, allow". Many access control mechanisms thus allow the users to override their privileges to provide effective care. At the first glance, it may seem as a good

solution but statistics have shown that 99% of the doctors had overridden their privileges while only 52% of them were required to do so [10]. Thus, this break the glass (BTG) policy is exploited almost every time which renders the whole architecture developed for providing security and privacy useless. There are many avenues for research in information access control such as new frameworks for establishing access control [11–13], new human identification algorithms [14–16], new security assessment techniques [17] and others [18,19]. We will be focusing on more generalized algorithms and models covering wide ranges of techniques available today.

In a nutshell, threats relating to an access control system arise from the following:

- Vast multitude of users accessing or modifying data with various permissions.
- Granular control that needs to be provided to reduce the use of overriding privileges.

9.3.2 Statistical disclosure control

In healthcare sector, it is often imperative to share patient data outside the perimeter of the closed information system for larger interests of various stakeholders involved with public health. While this data may be used for the greater good such as research of antibiotic for a new virus, it could also contain personal information that may be segregated and traced back to the patient it belongs to which as already stated, may lead to devastating consequences for the patient. Also, many a times, these types of databases are made public and cited in research papers for further scrutiny in the scientific community. Thus, virtually anyone, even without sufficient computer expertise or resources can access many of these databases. To avoid such repercussions, generally identifiable and sensitive information is masked before data are disseminated. Apart from obviously identifiable information like patient's name, address, contact, etc. that may be present in the data that were disclosed, there are other attributes that if grouped could act as a primary key in distinguishing and thus linking the data back to its owner.

However, it has also been argued that it is not possible to completely sever the link between the patient's data and its identifier. Also, as much as this link can be misused by malicious entities, it is also necessary for other purposes such as correcting an erroneous entry or establishing the credibility of the data to prevent fraud.

Data disclosure in these situations must satisfy two opposing purposes, that is, protecting the privacy of the individual while maintaining the maximum usability of the data. The former is also known as *disclosure risk* which as the name suggests relates to the privacy risks that an individual may be exposed to, due to this disclosure. The latter is also known as *information loss* which as the name suggests attributes to the information loss as more and more information is masked that reduces the risk of linking the data back to the individual. Thus, data disclosure for purposes other than directly related to the patient, may be a precarious preposition to handle.

In a nutshell, data disclosures must handle the following to minimize threats:

- Minimizing disclosure risk
- Minimizing information loss

9.4 Models and algorithms

9.4.1 *Information access control*

9.4.1.1 **Role-based access control**

In any organization, the data stored may be related to the end user. However, since many different entities apart from the end user may need to interact with the data, an access control system made on the basis of data ownership may not prove to be efficient. Instead, most organizations restrict access based on the ways a particular entity may be allowed to interact with the data. Access control system where decisions are performed based on the role of a particular entity are commonly known as role-based access control (RBAC) [20].

RBAC is one of the most popular access control mechanisms. RBAC works on the basis of the role a person is performing at a particular organization and because most organizations have already laid out specific functions of a role or a position needs to satisfy, it becomes very easy to integrate RBAC with the organization. For instance, a hospital has roles like doctor, nurse, pharmacist, etc. Here, the functions that the roles are allowed to perform are already known. A doctor is allowed to read and write prescriptions of a patient while a pharmacist is only allowed to read and execute the prescription. Also, when it comes to security and privacy, an organization usually needs to follow policies of a higher-level organization. For instance, in case of a hospital, an organization needs to follow HIPAA guidelines while implementing a health information system. It becomes very easy to follow regulations when access rights can be centrally controlled and maintained. In case of RBAC, this job is done by the system administrator. A RBAC system is normally concerned with both the information and the operations performed on it rather than just the access to the information. This helps RBAC to keep the data integrity in check as data are modified in form of operations performed on it. For instance, a cashier doesn't directly write the balance of the account. Instead, she invokes an operation that executes the transaction. Even though, the cashier has write-access to the data, she cannot simply overwrite previous transactions. This is because she performs her functions in form of a predefined operation which will not allow her to so. Thus, RBAC in a way helps to maintain the data integrity.

In RBAC, a *role* can be thought of as the set of operations it is allowed to perform. These operations are also known as *transactions*. The system administrator allocates the transactions to roles. Each transaction can be thought of as a procedure of operations that are performed to execute or complete the transaction. Here each role is also related to the individuals that perform those roles. It is also possible to segregate binding between transactions and the objects allowing finer control over the permissions. Thus, RBAC can be described as a many-to-many relationship between users, roles, permissions, and objects as shown in Figure 9.2.

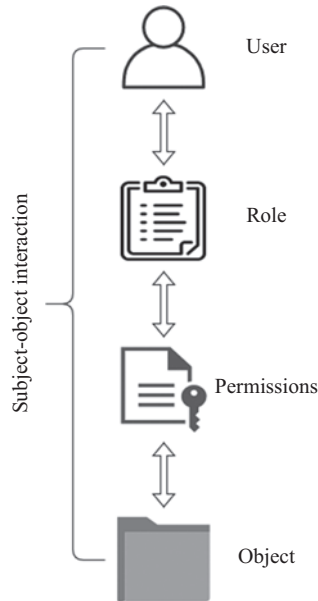


Figure 9.2 Many-to-many relationship between user, role, permission and object

It should also be noted that the login procedure is not considered as a transaction in RBAC. In other words, a login procedure which authenticates a user may be implemented separately. This gives flexibility to the organization if they feel the need to upgrade their authentication process.

RBAC also provides several other benefits such as separation of benefits. Since RBAC allocates transactions to roles, it is possible to assign some transactions to different users such that no user has two or more transactions that may give her an opportunity to commit fraud. Furthermore, since RBAC works on principle of least privilege, that is, “need-to-know” principle, it increases security and privacy.

However, just like any other model RBAC has its downfalls. Since RBAC is based on roles, organizations with large number of roles may lead to *role-explosion*. Also, RBAC isn’t well suited to manage individual rights.

9.4.1.2 Contextual role-based access control

The traditional RBAC model proves to be sufficiently functional for fulfilling access control requisites at a corporation level. It is able to provide appreciable level of granular control over access policy of different users performing sufficiently large number of roles. Moreover, RBAC employs a “need-to-know” strategy providing high information privacy and security. Furthermore, its compatible with Health Insurance Portability and Accountability Act of 1996 (HIPAA) [21].

However, unlike other information systems, health information systems need to be able to handle exceptional cases. Since the primary goal of an HIS is to provide best service to the patient as possible, there are cases where privileges need to be escalated so that patient's data could be accessed. For instance, it would be highly illogical and injudicious to prevent a physician from accessing EHR's of a patient in a life-threatening situation all because the physician doesn't have the required authorizations. Traditional RBAC allows this exception but is mostly misused or rather used in cases where there was no need. To provide better information privacy and security and yet handle this exceptional cases, Motta *et al.* have presented an approach also known as contextual role-based access control [22].

A contextual role-based access control or just CRBAC provides better information security and privacy by including contextual requests for authorizations. Unlike RBAC, it has the potential to define finer access control policies that takes the current situation into account. In other words, it provides more flexibility in defining access control policies.

In case of RBAC, authorizations can be defined as the transactions or operations that are allowed for a particular role. Mathematically, it can be represented as a tuple of five values, that is

$r, pt, opr, obj, at \rangle$ where,
 r is the role of the user,
 pt is the privilege type,
 opr is the operation,
 obj is the resource or object under consideration and
 at is the authentication type.

Thus, for instance $\langle Pharmacist, +, execute, prescription, strong \rangle$ means that a *pharmacist* is allowed to perform the transaction *execute* on the object *prescription* and this is a *strong* type of authorization.

In case of CRBAC, contextual information is used in authorization expressions. This information is in the form of contextual variables* that describes the current scenario. Different types of variables are available that describe the current situation of different entities that might affect the overall decision of the physician. For instance, a variable like *patientCntx* may describe the patient or *userCntx* may describe the user. These variables may have different attributes associated with them. For instance, *userCntx.takes_care_of* may define the number of patients under the user's care. A rule consists of different contextual variables operated on by logical operators such as relational, boolean, arithmetic operators, etc. For instance, the following rule will allow a *physician* to perform the *read* transaction on the object *medRecords* if the patient id (*apatientCntx*) is in the list of patients treated by the physician.

```
exp-abs(apatientCntx) {
    apatientCntx in patientCntx.in_patients
}
```

Therefore, in a CRBAC model, authorization will be represented in the following manner.

```

⟨ Physician,
  exp-abs(apatientCntx) {
    apatientCntx in patientCntx.in_patients
  }, read, medRecords, strong ⟩

```

*It should be noted that the variables actual name in the implementation of CRBAC may differ.

This model is mainly aimed at large organizations where the traditional RBAC might not prove that helpful. Like RBAC, CRBAC also works on “need-to-know” basis. Moreover, CRBAC, segregates the complex authorization logic and makes it more understandable. Furthermore, since authorization in urgent or exceptional cases is better understood in form of contextual rules, the misuse of privilege escalation is reduced as well as could be analyzed in future for further improvement and inconsistencies. Since, patients now have more detailed reasons as to why privileges were overridden, it makes up for a more transparent system.

However, just like any other model CRBAC has its pitfalls. Firstly, the authorization rules are complex and thus the implementation is much more complex than that of RBAC. Also, in RBAC conflicts between authorization could be identified and removed much more easily than in CRBAC. Apart from CRBAC, there are many extended or advanced versions of RBAC that provide different capabilities at the cost of simplicity.

9.4.1.3 Tag-based data model

So far, we have discussed models that are based on the interactions that different entities of an organization are allowed to have with the data. However, this doesn’t consider the fundamental fact that the data are of the patient and thus should be owned by her. In other words, any access to the data shall not occur without the consent of the patient. The primary goal of these types of models is to alleviate the privacy concerns of the patient. One such model was the eConsent or Electronic Consent model that was developed with the aim of protecting the privacy of the patient by transmitting data through anonymous transmission protocols by using the notion of “placeholders” [23,24]. This tag-based data model extends the eConsent model to overcome its weaknesses [25].

The elementary unit of information in this model is an electronic record or *eRec*. EHRs such as X-ray, prescription, blood test report, etc. can be stored in a single *eRec*.

One or more policy tags or *eTags* are connected with each electronic record. Each *eTag* has the fields as shown in Figure 9.3. The first field is the category field.

<Category Type, Value>	<eCo>

Figure 9.3 Structure of *eTag* [24]

It is a tuple of two quantities. The former is the category type which dictates whether the category is related to facility, family, or patient. The latter is referred to as the value of the category which contains the information about the actual category like heart, head, AIDS, etc. The rights are stored in the second field which is also known as electronic consent or *eCo*.

The *eRecs* and the *eTags* are related to each other in a many-to-many relationship as shown in Figure 9.4. *eTags* may be of three different types. First type is used to signify record-specific policies. Second type is only used to specify information about categories. The third type contains both nonnull category and nonnull policy and is used to signify a set of policies for a set of records. The *eCo* or the electronic consent category not only defines the access policy but also the transfer policy. These are written in policy languages such as XACML and OMA 2.0, respectively. Moreover, a timestamp is attributed with each policy so that it may be used for audit and conflict resolution. Furthermore, just like *eRecs* are considered as sensitive information and will not be accessed by anyone until and unless the access policies are satisfied, *eTags* are also considered sensitive. This would otherwise be considered as a poorly designed system.

Both the access and transfer policies are defined at the patient, family, and the facility levels. They may also be defined for different categories such as heart, AIDS, etc. At each level, a default policy is also defined. These policies may take priorities with each other. As it may be readily apparent, the patient policy takes the top priority followed by family, facility, and optionally categorical levels. Although two hospitals may follow the same regulation, they may implement it differently in form of various sets of policies and their mappings.

For instance, a patient may decide to only let his personal doctor (Dr. Bob) know the results of his blood test while his family may decide that result of their

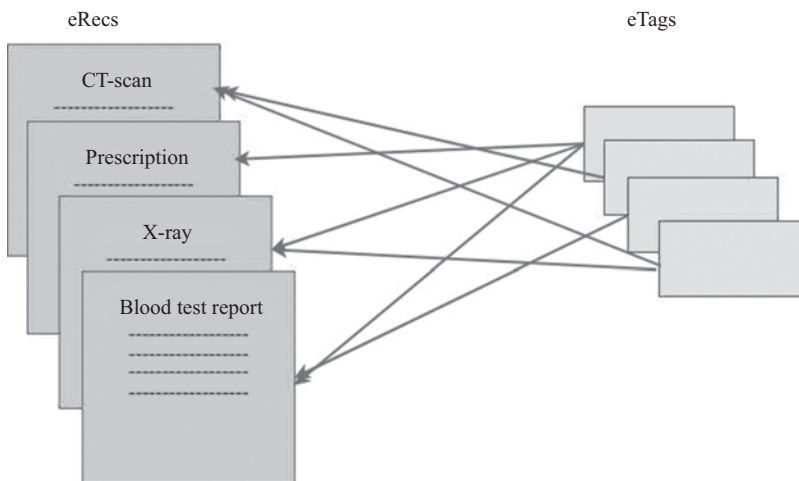


Figure 9.4 Many-to-many relationship between *eTags* and *eRecs* [24]

blood test will be known by their family doctor (Dr. Alice). As the patient's policies takes priority, the blood test of the patient will be accessible to Dr. Bob and herself only. Similarly, a hospital may decide to give access to blood test results to only the lab staff.

As one can see, hospital's policies will resemble the role-based access protocols. Thus, like RBAC, this model is capable of controlling access rights based on roles of individuals in an organization. Moreover, it is able to define access and transfer control policies on the basis of not just role-based categories but also many others. Furthermore, it is much more flexible in policy making than the traditional RBAC model. One major advantage of this model is that it gives full power to the patient. Some other advantages include use of nonhierarchical structure, implicit conflict resolution, definition of default policies, etc. The only major disadvantage would be increased complexity in implementation and maintenance of such system.

9.4.1.4 Privacy management architecture

Nowadays, there are various laws and regulations surrounding privacy and security of data in a health information system like the Personal Data Protection Law [26] of Japan, Health Insurance Portability and Accountability Act (HIPAA) of the United States [27], and the Personal Information Protection and Electronic Documents Act of Canada [28]. Although these laws and regulations have very strict privacy policies, it may not have the intended result. It has been shown that strict privacy policies don't necessarily convert into equally sufficient patient privacy protection [29]. This is mainly because the framework and mechanisms implemented for protected privacy are often bypassed by privilege escalation. Nowadays, outmaneuvering the policies protecting privacy has become the norm and the norm has become the exception. According to HIPAA, only minimum necessary information must be disclosed for a specific purpose. However, these purposes are more likely defined to be very vague. Although this may not be done with hostile intentions, but these lax definitions render the enforcement of these laws worthless. Moreover, due to an enormous increase in number of departments, number of healthcare professionals and number of disciplines in medicine, organizations are facing high amount of complexity in rigidly defining functions of different positions in an organization. These days, many entities are involved in offering their service to provide care to just one client, that the fine line between the functions of different roles in an organization has blurred over the years. Now, for instance, the whole medical staff may be able to access a patient's data. The "need-to-know" factor has diminished over the years. A little attention has been given to this component of access control. With the purpose of overcoming these hurdles, PRIVacy Management Architecture (PRIMA) was developed [30].

PRIMA seeks to systematically reduce the differences between the privacy policy written and the policies being used. It does this by analyzing existing information in the system and adapting the policies that the system may need to develop into.

PRIMA consists of three major components as shown in Figure 9.5. These are *privacy policy definition*, *policy refinement*, and *audit management*. Privacy policy

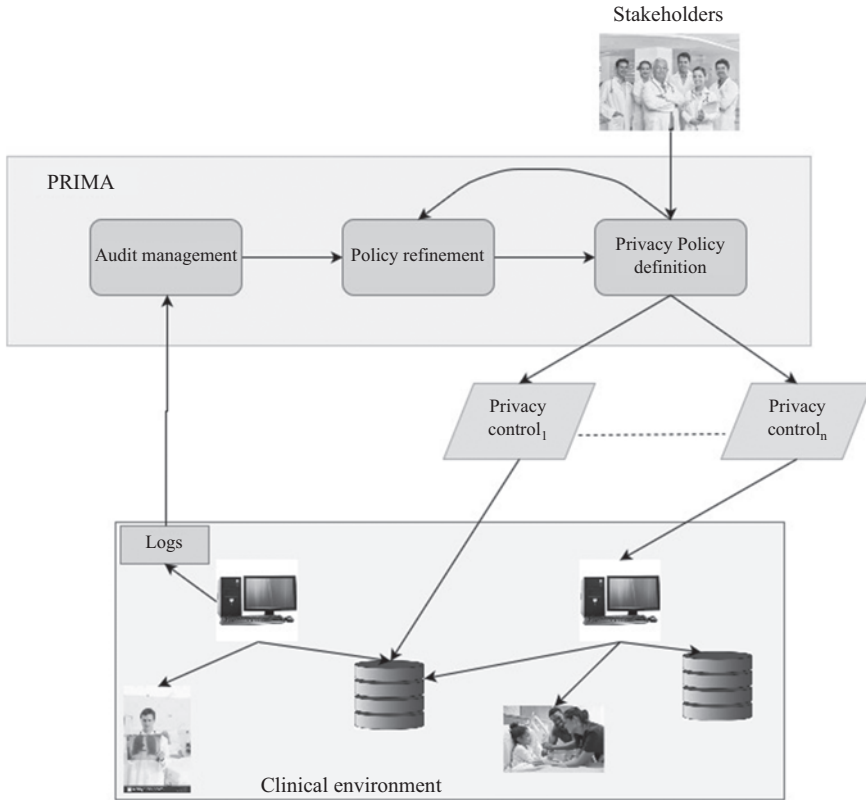


Figure 9.5 The PRIVacy management architecture (PRIMA) [30]

definition refers to the “ideal” policy definitions that are created and formalized by the group of stakeholders which may include the patients, healthcare professionals, payers, etc. These are the policies that are initially decided upon before they are outmaneuvered and rendered useless. At a very conceptual level, any privacy policy could be utilized by PRIMA as long as it can be embedded with the health organization’s workflow. Audit management component of PRIMA is the information aggregator which PRIMA may use for future analysis. At first glance, it may seem that this component is already present in most systems (for bug detection). However, there are some problems regarding this approach. Firstly, since audit system will perform one of primary duties, it may decrease system’s efficiency and increase storage requirements. Secondly, most audit systems are only utilized in case of red flags. Thirdly, in most systems not all the information is logged which may not be enough for ensuing analysis. PRIMA uses HDB Compliance auditing to realize most of the above requirements of audit management. Policy refinement refers to the procedure or the set of procedures that are executed to refine the privacy policies to better suit the needs of the health

organization and its patients. The algorithm works on a feedback loop between the actual and the ideal policies taking the policy store (P_{PS}), the policies in the logs (P_{AL}) and the privacy policy vocabulary (V) as inputs. As the requirements of a health organization constantly changes, the PRIMA model needs to be trained again after reasonable amount of information is aggregated.

PRIMA has many advantages. First of all, it solves the problem of misuse of break-the-glass (BTG) policies. It also creates more realistic policy definitions without hampering or slowing down the health organization's workflow. Most of all, it provides improves the privacy of the patient.

9.4.2 Statistical disclosure control

9.4.2.1 Pseudonymization

The models that we have discussed so far protect the privacy of an individual by restricting access to the patient data. Then, access for a certain portion is only given to authorized personnel. However, there are some other ways by which not only will the data be protected in its primary use, that is, providing care to the patient but also in secondary uses such as for medical research. The data of a patient can be divided broadly into two parts. The first part will consist of actual medical data such as blood reports, X-rays, CT-scans, etc. The second part will consist of other information such as name of the patient, address, and contact. This type of information can be used to identify or link the patient's identity with her data. It should be noted that as long as unauthorized entities cannot trace medical data back to a patient's identity, her privacy is protected. Therefore, several models or algorithms try to sever this link so that although the data may be public or accessible by an entity, she shall not be able to trace it back to the patient's identity. For instance, a technique called *anonymization* involves completely separating patient's identification data with her actual medical data. This type of technique shall provide utmost privacy and the data could be used for secondary purposes. However, since the data can never be traced back to the patient, the validity of research data cannot be verified. Moreover, the patients may not be able to realize the results of these medical researches. Another approach is called *depersonalization* which involves removing as much identification data as needed to prevent any linking between the data and the patient's identity. Reidl *et al.* suggested a better approach, known as *pseudonymization* [31].

Pseudonymization refers to removal of identification data and addition of an identifier that may later be used to link the data back to the patient. This identifier is known as *pseudonym*. This technique has several advantages over the conventional ones. First of all, it provides access control at an encryption level, that is, unlike a traditional RBAC which simply restricts access to data, the data will remain unintelligible or unusable unless the user is authorized to access the data. Secondly, the data could be used for secondary purposes since the data could be only linked to the patient when it's authorized by the patient. Thirdly, if a patient uses enough pseudonyms, it would be implausible to do any kind of profiling which may expose the identity of the patient. Lastly, this mechanism also provides recovery techniques in case the user forgets or loses her security key.

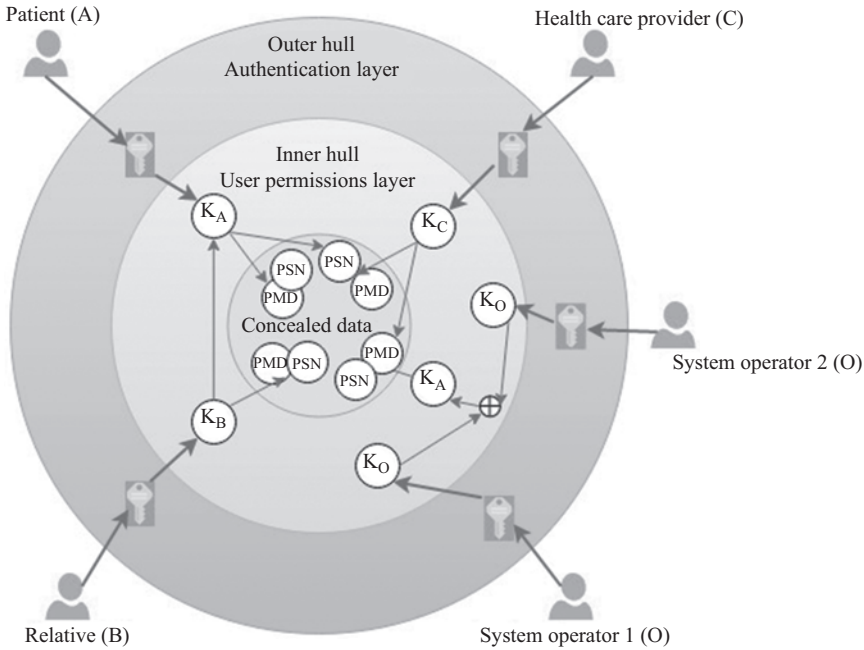


Figure 9.6 Pseudonymization layered model [31]

Pseudonymization as shown in Figure 9.6 has a layered model with at least three rings of protection. There are many entities interacting with the model such as the *patient*, *healthcare provider*, *relative*, and *system operators*. Every layer introduces another level of encryption. For instance, a key K_i of a layer L_i would be encrypted with a key K_{i+1} of its enclosing layer L_{i+1} . A *pseudonym* is linked with each entry in the medical database. The pseudonym is generated using an algorithm on the identification data of the patient which uses the key of the innermost layer. Any user which needs to access the data must start at the outermost layer. The user will start by using her private key to decrypt the key in the user permission layer. For instance, as shown in Figure 9.6, once the patient gets the key K_A , she can use it to select a portion of data she wants to reveal by regenerating the pseudonym using her personal data. Apart from the patient herself, anyone who is authorized to access the data needs to be provided with her own key to enter the user permissions layer. The concept of unobservability may be implemented by using different pseudonyms for different transactions. For instance, a patient may choose to create a new pseudonym whenever he visits a physician. This way, even when the data are not necessarily encrypted, no link could be established between two sets of her own data. In addition to unobservability, a patient can easily grant or revoke access of another user to her data by sharing or changing security key. The recovery mechanism could be implemented in many ways. The patient may choose to share her security key with a relative which most likely be able to recover the data in case

the patient has lost her security key. It is also possible to share a shared-secret to more individuals where they need to act unanimously to access someone's data. So, for instance, k operators out of n operators may need to act unanimously to unveil data of a patient. This reduces the risk of misuse if some operators conspire to act maliciously.

This pseudonymization model aims to seek a balance between privacy and the efficiency of the services offered. It provides great deal of privacy at encryption level. However, obviously this makes the system more complex and resource intensive which is obviously a trade-off between privacy and efficiency of the system.

9.4.2.2 p-sensitive k-anonymity property

Although the data of a patient are solely hers and she is the ultimate owner of the data, sometimes it is necessary to disclose that data in favor of greater good. Many patients provide their data for research to trusted healthcare organizations. So, at first glance, it may not seem as big of a risk. However, since various organizations are involved simultaneously in medical research, access control over that data is difficult to impose and thus even a single weak link in the chain make expose the entire database to plethora of risks. However, the benefits of doing medical research on huge collection of accurate patient data far outweigh the risks of privacy invasion that an individual may take. Even so, this doesn't mean that the disclosure should be done with the risk of exposing someone's privacy. Therefore, many laws and regulations require certain baselines to be satisfied before the data are released for research. For instance, generally these regulations require that attributes such as names, contacts, etc. be removed before the data are released for research. These techniques enforced by laws and regulations are rudimentary at best as there are many advanced techniques which may be utilized to profile a patient. For instance, Pin Code, Gender, Birth Date, etc. that are normally left in these databases can be cross-referenced with known public databases may reveal identities of many patients.

However, there are many techniques that can be used to increase privacy of these patients. One of them is the *k-anonymity* property. If this property is satisfied by a database, then any kind profiling cannot trace back to a group of individuals less than k in size. Although this property is able to prevent *identity disclosure*, it is not able to prevent another type of disclosure known as the *attribute disclosure*. Another property p-sensitive k-anonymity property proposed by Truta *et al.* extends upon the k-anonymity [32,33].

The attributes of the patient data that do not directly relate to his medical condition but instead is related to her personal information could be divided into three categories. *Identifier attributes* are attributes which directly relate to an individual's identity such as name, address, social security number, etc. These attributes are generally removed from the final database. *Key attributes* are attributes that may be known to a malicious entity and if grouped together, may uniquely identify the individual. These attributes generally remain in the database. Finally, *confidential attributes* are attributes that are assumed to be unknown to a

malicious entity and are normally removed from the final database. If a database satisfies the *k-anonymity* property, then any combination of key attributes will be found to be in relation with at least *k* entries in the database. For instance, the database below satisfies *2-anonymity* property where key attributes = { *PinCode*, *Gender*, *Age* }.

It can be seen that for every different combination of the key attributes, there are at least two entries related to them, that is, the database as shown in Table 9.1 satisfies the *k-anonymity* property. While, this is able to prevent *identity disclosure* (since no combination of attribute can relate to a single individual), it may not be able to prevent *attribute disclosure*. Attribute disclosure usually occurs when a malicious entity discovers new attributes about the victim's identity. For instance, if the malicious entity uses the information available publicly, shown in Table 9.2 and the knowledge that the age is generalized in order of 10, she may be able to discover new attributes. Using the information shown in Table 9.2, although a malicious entity may not be able to deduce as to which entry does the group of attributes { 50, 110078, M } related to, that is, Samuel or Elliot. She can, however, deduce that both of them have Asthma. So, although, no *identity disclosure* occurred, an attribute or new information was discovered (*attribute disclosure*). This can be prevented by satisfying *p-sensitive k-anonymity* property. This property is satisfied by a database if and only if when no combination of *key attributes* can trace back to a group of size less than *k* (*k-anonymity*) and the confidential attributes have at least *p* unique values for every combination of *key attributes* (*p-sensitivity*). Similar to *k-anonymity*, *generalization* and *suppression* methods can

Table 9.1 *Patient database satisfying 2-anonymity property*

Age	Pincode	Gender	Medical condition
40	110078	M	Blood cancer
30	110078	F	Lung cancer
30	110078	F	Heart disease
50	110078	M	Asthma
50	110078	M	Asthma
40	110078	M	HIV

Table 9.2 *Public information*

Name	Age	Gender	Pincode
Samuel	59	M	110078
Guinevere	37	F	110078
Alex	41	M	110078
Elliot	59	M	110078
Tanya	33	F	110078
Derek	41	M	110078

be used to mask the database to satisfy the p -sensitivity property. In addition to this, generalization lattice can be utilized to achieve the p - k minimal generalization.

9.4.2.3 Microaggregation

When data are shared for research purposes, it should be done in such a way that does not disclose identifiable information of an individual. Ordinarily, two types of data are disseminated for statistical analysis. First type is the tabular data while the second type is microdata set. A microdata set is a collection of entries of data vectors that relates to individual entities such as persons, corporations, etc. Each data entry in microdata set consists of two types of variables, that is, *key variables* and *sensitive variables*. *Key variables* consist of attributes that could identify an individual. For instance, a key variable could be an attribute that directly identifies the individual such as social security number. *Sensitive variables*, however, consists of attributes that must remain confidential. For instance, salary information may be held confidential. Since both of these variables carry information about an individual, microdata sets should be defended from unwanted disclosure. Information disclosure is also of two types. First is the *re-identification disclosure* which may lead to identification of the individual while the second is *prediction disclosure* which may not lead to identification of the individual but predicts the value of a sensitive variable of that individual. Therefore, disclosure should be done in such a way that the probability of unwanted disclosure is very low and at the same time, the datasets still retain their statistical information.

Microaggregation is one such method by which unwanted disclosure is prevented [34]. The logic behind microaggregation is that if the data vectors of the dataset relate to a collection of k or more individuals, then confidentiality of the individual is preserved. So, in microaggregation, g groups consisting of not less than k individuals are formed. Then, mean of every group is calculated and is used as a substitute for each of the original values. After this step, the output data vectors could be disseminated. However, obviously data entries could not be selected at random otherwise, the statistical property of the dataset would be lost and it will be rendered useless. Therefore, the segregation of the data vectors would be done in such a way that minimizes the information loss as much as possible. As is evident, the information loss will be minimum when the data vectors belonging to a particular group are similar to each other. In other words, groups should contain data vectors that are similar to each other.

The similarity between two data vectors could be calculated as the Cartesian distance between them when the vectors are considered as points in n -dimensional space where n is the dimension of the data vector and its values as the coordinates in different dimensions respectively. For instance, as shown in Figure 9.7, the points A and B are more similar to each other than points A and C . Therefore, if $g = 2$, then the groups should be formed as shown in Figure 9.7. The optimal segregation strategy would be such that every group consists of most similar data vectors. Mathematically, optimal segregation strategy would maximize intragroup uniformity by minimizing the sum of squares (that is defined as the sum of square of difference between any data vector point and group specific mean vector point).

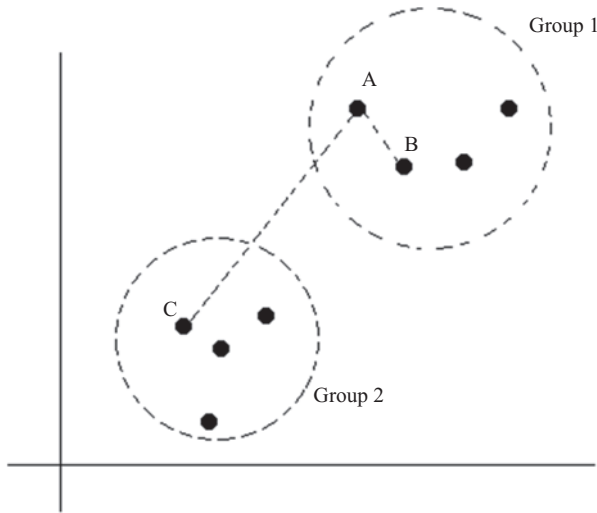


Figure 9.7 Representation of data vectors of size 2

Although an optimal microaggregation strategy, might yield great results such as minimized disclosure risk and information loss. However, this k -partition problem is related to the conventional minimum sum of squares clustering (MSSC) problem which is an NP Hard problem. Thus, instead of correctly solving the problem an approximate solution is calculated from heuristic approaches of microaggregation such as univariate microaggregation based on ward hierarchical structuring, genetic approach to univariate microaggregation, multivariate fixed-size microaggregation, etc.

9.5 Conclusions and future directions

In this chapter, we have explored several aspects of healthcare and how a well-designed information system could revolutionize healthcare services while potentially saving billions of dollars. We have also seen the crucial role that information security and privacy plays in HISs. A HIS or EHR cannot be implemented without giving special thought to information security and privacy infrastructure. It is also evident that HIS has peculiar problems regarding information privacy and security and thus requires innovative and custom solutions for them. Furthermore, since the primary function of an HIS is to provide best care possible to the patient, there has to be a trade-off between the levels of security and privacy and the efficiency of the system.

Threats to information security and privacy: Threats to information security and privacy are one of the major hurdles as to why HIS has yet not been implemented in every healthcare institution. Although we have explored different types of threats in previous sections, the amount of research backing it up is quite

insufficient. There is still lack of systematic analysis of threats to information security and privacy in healthcare information. In presence of a detailed threat model and its classification, new and meticulous algorithms and models can be developed.

Privacy concerns: Although patients are very sensitive about who can access their medical data, they understand that their data may be shared among healthcare professionals to provide them with best care possible. Also, patients with very sensitive medical conditions such as HIV are still skeptical and hesitant to share information. Moreover, many patients dismiss the idea of sharing their information with third parties. Since most of the privacy policies revolve around privacy concerns of patients, it is beneficial to continuously analyze the ever-changing opinions of patients.

Laws and regulations: Many governments have passed several legislations regarding the medical data of patients. Some of them are Personal Data Protection Law [26] of Japan, Health Insurance Portability and Accountability Act (HIPAA) of the United States [27], and the Personal Information Protection and Electronic Documents Act of Canada [28]. These regulations not only enforce on how and who can access health information but also defines baselines that must be satisfied before a health information system is implemented. For instance, HIPAA requires three safeguards in place, before public's valuable and sensitive health information is stored on it. Although laws and regulations are keeping in pace with the changing requirements of patients, the strictness of policies doesn't always translate to equally better information security and privacy for the patients. For instance, it was discussed in the 9.3.1 section, that BTG policies are used by healthcare professionals all the time which renders enforcement of laws useless. Therefore, laws and regulations need to make better policies that can prevent misuse of exception handling.

Information access control: Information access control is one of the most important mechanisms that need to be implemented for any technological solution. Therefore, there are plenty of complex and more secure access control mechanisms for health information systems. In previous sections, we discussed many such models like the traditional RBAC model and CRBAC model. We also explored some unconventional models such as tag-based data model where consent of the patient gets the attention it deserves. Another model was PRIMA which analyses past access control logs to create more practical and secure privacy policies. Although we have discussed many technological solutions for access control in health information, very few models have been developed which could better handle the access on different attributes of one's health information. In addition to this, very few models take into account human errors and their behaviors. Also, there are not many studies in cost-effective information access models. Future research should be directed toward these types of models.

Statistical disclosure control: The secondary use of health information is to conduct medical researches. Since healthcare data of millions of people are disposable in a click, lots of accurate data are available for medical research. However, it becomes equally important to protect the privacy of millions of people

as most of these datasets used for medical research may be available to the whole public or may be accessible by a lot of organizations. Therefore, many models have been developed to mask the patient's data such that the data used for medical research. We discussed the pseudonymization architecture and the p -sensitive k -anonymity property. However, most of the research in this field is very theoretical and may be inefficient in a real scenario. Therefore, future research should focus on real-world algorithms and quantitative analysis of the effects that these complex models produce in contrast to simple models.

Global health information system: As more and more healthcare institutions are implementing health care information, it is imminent and beneficial to construct a global health information system. This not only will allow unprecedented access to patient's data from any corner of the world but also increase efficiency and interoperability of different departments and different healthcare institutions. However, since healthcare data are so complex it is difficult to create an interoperable system. Also, since many hospitals have their own proprietary health information data formats, an error-free conversion is essential. Many new privacy and security threats will arise from implementing such a system. Although we have not discussed these threats above, it is evident that such a system will be implemented sooner or later. Thus, future research directions should be toward development of a global health information system.

We trust that this chapter has provided useful insights to anyone who wants to build a health information system. Also, we hope that the recommended future directions will stimulate further research into this field.

References

- [1] Hillestad R., Bigelow J., Bower A., *et al.* (2005). "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs," *Health Affairs*, Vol. 24, No. 5, pp. 1103–1117.
- [2] Applebaum P.S. (2002). "Privacy in psychiatric treatment: threats and response," *American Journal of Psychiatry*, Vol. 159, pp. 1809–1818.
- [3] Ponemon Institute LLC (2017). "Fifth annual study on medical identity theft." Available from URL: http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf [Accessed May 2019]
- [4] Heather L. (2017). "Survey: Patients Skeptical of Health IT Due to Privacy, Security Concerns," *HC Innovation Group*; Available from URL: <https://www.healthcare-informatics.com/news-item/cybersecurity/survey-patients-distrust-health-it-due-privacy-security-concerns> [Accessed May 2019]
- [5] Liu V., Musen M.A., and Chou T. (2015). "Data breaches of protected health information in the United States," *JAMA*, Vol. 313, No. 14, 1471–1473. doi:10.1001/jama.2015.2252
- [6] Jouini M., Rabai L.B., and Aissa A.B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, Vol. 32, 489–496. doi:10.1016/j.procs.2014.05.452

- [7] Appari A., and Eric Johnson M. (2010). "Information security and privacy in healthcare: current state of research," *International Journal Internet and Enterprise Management*, Vol. 6, No. 4, pp. 279–314.
- [8] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) [online]. 2019. Available from URL: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/> [Accessed May 2019]
- [9] Mario S., and Back A. (2014). "Information security," *Information Management and Computer Security*, Vol. 22, No. 3, 279–308
- [10] Røstad L., and Edsburg O. (2006). "A study of access control requirements for healthcare systems based on audit trails from access logs," *Proceedings of the 22nd Annual Computer Security Applications Conference*, Miami Beach, FL, pp. 175–186
- [11] Kumari A., Tanwar S., Tyagi S., and Kumar N. (2018). Fog computing for Healthcare 4.0 environment: opportunities and challenges," *Computers & Electrical Engineering*, Volume 72, 2018, Pages 1–13.
- [12] Vora J., Tanwar S., Verma J.P., *et al.* (2018). BHEEM: a blockchain-based framework for securing electronic health records," *IEEE Global Communications Conference (IEEE GLOBECOM-2018)*, Abu Dhabi, UAE, December 09–13, 2018, pp. 1–6.
- [13] Vora J., Tanwar S., Tyagi S., Kumar N., and Rodrigues J.P.C. (2017). FAAL: fog computing-based patient monitoring system for ambient assisted living," *IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom-2017)*, Dalian University, Dalian, China, October 12–15, 2017, pp. 1–6.
- [14] Hathaliya J., Tanwar S., Tyagi S., and Kumar N. (2019). Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach," *Computers & Electrical Engineering*, 76, pp. 398–410.
- [15] Tanwar S., Obaidat M.S., Tyagi S., and Kumar N. (2019). Chapter 10: Online signature-based biometrics recognition," M. S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG, pp. 255–285.
- [16] Tanwar S., Tyagi S., Kumar N., and Obaidat M.S. (2018). Chapter 21: Ethical, legal, and social implications of biometrics technologies," In M.S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG, pp. 535–568.
- [17] Tanwar S., Thakkar K., Thakor R., and Singh P.K. (2018). M-Tesla-based security assessment in wireless sensor network," *International Conference on Computational Intelligence and Data Science (ICCIDS 2018)*, NorthCap University, Gurugram, April 07–08, 2018.
- [18] Vora J., Devmurari P., Tanwar S., Tyagi S., Kumar N., and Obaidat M.S. (2018). Blind signatures based secured E-healthcare system," *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, July 11–13, 2018, pp. 177–181.

- [19] Vora J., Italiya P., Tanwar S., *et al.* (2018). Ensuring privacy and security in e-health records,” International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018), Colmar, France, July 11–13, 2018, pp. 192–196.
- [20] de Carvalho Junior M., and Bandiera-Paiva P. (2018). Health information system role-based access control current security trends and challenges. *Journal of Healthcare Engineering*, [online] 2018, pp. 1–8. Available from <http://downloads.hindawi.com/journals/jhe/2018/6510249.pdf>. [Accessed May 2019]
- [21] Department of Health and Human Services (1998). “Security and electronic signature standards,” Federal Register, Vol. 63, pp. 43, 241–43, 280.
- [22] Motta G.H.B., and Furuie S.S. (2003). “A contextual role-based access control authorization model for electronic patient record,” IEEE Transactions on Information Technology in Biomedicine, Vol. 7, No. 3, pp. 202–207
- [23] Coiera E. (2004). e-Consent: the design and implementation of consumer consent mechanisms in an electronic environment. *Journal of the American Medical Informatics Association*, Vol. 11, No. 2, pp. 129–40. doi:10.1197/jamia.M1480.
- [24] This work is completed as part of CeNTIE project that is supported by the Australian Government through the Advanced Networks Program of the Department of Communications, Information Technology and the Arts.
- [25] Nepal S., Zic J., Jaccard F., and Kraehenbuehl G. (2006). “A tag-based model for privacy preserving medical applications,” in Grust T., Höpfner H., Illarramendi A. *et al.*: Current Trends in Database Technology – EDBT Workshop, pp. 433–444.
- [26] Ministry of Internal Affairs, Communications Information, and Communications Policy. Personal data protection law.
- [27] Health Insurance Portability and Accountability Act, U.S. Department of Health and Human Services. 2017. Your rights under HIPAA [online] Available from URL <http://www.hhs.gov/ocr/hipaa> [Accessed May 2019]
- [28] Office of the Privacy Commissioner of Canada. (2019). Personal Information Protection and Electronic Documents[online]. Available from URL <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/> [Accessed May 2019]
- [29] Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). (2004). Break-glass an approach to granting emergency access to healthcare systems.
- [30] Bhatti R., and Grandison T. (2007). “Towards improved security policy coverage in healthcare using policy refinement,” In Jonker, W. and Petkovic, M. (eds.), *Lecture Notes in Computer Sciences*, Vol. 4721, pp. 158–173.
- [31] Reidl B., Neubauer T., Goluch G., Boehm O., Reinauer G., and Krumboeck A. (2007). “A secure architecture for the pseudonymization of medical data,” Proceedings of 2nd International Conference on Availability, Reliability and Security, Vienna, Austria, pp. 318–324.

- [32] Truta T.M. and Vinay, B. (2006). "Privacy protection: p-sensitive k-anonymity property," Paper presented at the 2nd International Workshop on Privacy Data Management, 8 April, Atlanta, GA.
- [33] Sweeney L. (2002). "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal on Uncertainty, Fuzziness, and Knowledge-based Systems*, Vol. 10, No. 5, pp. 571–588.
- [34] Domingo-Ferrer J., and Mateo-Sanz J. (2002). "Practical data-oriented microaggregation for statistical disclosure control," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 14, No. 1, pp. 189–201.

This page intentionally left blank

Chapter 10

Safety measures for EHR systems

Deverajan Ganesh Gopal¹ and Udhayakumar Hari Haran²

The Health Information Technology for Economics and Clinical Health (HITECH) Act of 2009 called for the widespread adoption and implementation of electronic medical records (EMR) to improve care quality, avoid unnecessary cost, and promote patient safety as a cultural norm. An electronic health record (EHR) is the systematic collection of patient and population electronically stored health information in a digital format. EHR systems are designed to store data accurately and to capture the state of a patient across time. It eliminates the need to track down a patient's previous paper medical records and assists in ensuring data are accurate and legible. It can reduce data replication as there is only one modifiable file which means the file is more likely up-to-date and decreases risk of lost paperwork.

Sociotechnical models of EHR, EMR, CPOE, MAR, and eMar use point to complex interactions between technology and other aspects of the environment related to human resources, among others. Diverse stakeholders—clinicians, researchers, business leaders, policy makers, and the public—have good reason to believe that the effective use of EHR is essential to meaningful advances in health care quality and patient safety. However, several reports have documented the potential of EHRs to contribute to health care system flaws and patient harm. As organization with limited resources for care process transformation, human-factors engineering, software safety, and project management begin to use EHRs, the chance of EHR associated harm may increase. These include setting EHR implementation in the context of health care process improvement, building safety into the specification and design of EHRs, safety testing and reporting, and rapid communication of EHR-related safety flaws and incidents.

The most frequently mentioned security measures and techniques are categorized into three themes: administrative, physical, and technical safeguards. The sensitive nature of the information contained within electronic health records has prompted the need for advanced security techniques that are able to put these worries at ease. It is imperative for security techniques to cover the vast threats like

¹Department of SCSE, Galgotias University, Greater Noida, India

²Department of Information Technology, Galgotia College of Engineering and Technology, Greater Noida, India

substantial learning curve, confidentiality, security issues, lack of standardized terminology, system architecture, and indexing.

10.1 Introduction

There is a developing accord that far-reaching reception of electronic Healthcare records (EHRs) is fundamental to accomplishing numerous American medicinal services objectives, including enhanced consideration quality and patient well-being. Actual fact that the advantages of all around oversight EHRs may appear glaringly evident and are likely considerable, the general security and viability of EHR is not included [1,2]. Maybe a couple of EHR's hazards the board procedures have been distributed.

10.1.1 *Traditional record maintenance in EHR*

EHR comprises of a store of data concerning the wellbeing status of people. In an EHR, wellbeing records are made and oversight in advanced configurations [1]. An EHR of a patient can contain restorative history including activities, hospitalizations, meds, past symptomatic development, research facility results, radiology reports, and significant human services data [2,3]. It is a safe and solid wellspring of clinical data where wellbeing records can be securely shared.

The historical backdrop of clinical documentation depends on paper-based records, and they are awkward and inadequate [2]. Proficient information recovery is conceivable from EHR frameworks in manners that paper documentation cannot do [1]. Customary medicinal records have confinements in permitting a worldwide vision of the patient's wellbeing conditions. An EHR rather expects to accumulate wellbeing information, conceivably produced by various sources on various occasions and offers those, information with significant human services frameworks [4]. The sharing of medicinal services data between suppliers utilizing EHR has prompted enhanced results of consideration and diminished clinical blunders [1].

The achievement of a human services framework relies upon keeping up patient's trust. At the point when patients lose their trust in the protection of their wellbeing data kept by the suppliers, it prompts conceivably hazardous advances including patients not legitimately unveiling critical wellbeing data, and can even come full circle in customer's refusal to the EHR framework [2].

Appropriately structured EHR frameworks wipe out the need to bring down translations on paper and can well sort out doctor's work processes bringing about expanded proficiency and efficiency. The utilization of EHR frameworks has assisted the human services suppliers with a better trade of lab results, checks reports, and enhanced specialized technique with patients [3]. An all-around actualized human services framework will decrease the wasteful aspects and advance a superior social insurance. EHR guidelines are one of the basic building hinders for medicinal services change and a critical part that bolsters productive trade of data among suppliers and social insurance associations [5,6].

Proficient human services conveyance is tied in with giving consideration without the inefficient utilization of assets. Copy testing and endorsing can be diminished by the EHR's capacity to exchange understanding data consequently between medicinal services locales. Programmed updates will decrease blunders, enhance profitability, and advantage tolerant consideration [7].

The capacity of EHR to share data electronically gives a lift in quality in medicinal services the board. The fundamental objectives of EHR incorporate giving a safe, dependable, and proficient approach to enroll, accumulate, and process all the clinical information identified with the patient. Likewise, it bolsters the activities identified with the clinical practice and patient treatment [8]. At the point when ideally actualized, EHR holds a colossal potential advantage for medicinal services frameworks, and can upgrade how quiet information are recorded and sorted out. It is along these lines critical to study and discover the present issues in regards to EHR to make it progressively effective and helpful.

10.1.2 Electronic healthcare report

The arrangement of connected electronic data the executives subframeworks used to help coordinate patient consideration. The common place EHR is involved in a developing arrangement of interconnected programming applications including however not constrained to tolerant information vaults with connections from feeder frameworks, for example, research facilities, electronic correspondences among clinicians and patients, arrange the board frameworks (counting care arranging, arrange section, drug store arrange preparing, and documentation of prescription organization), and information input gadgets. Assorted affiliations' EHRs are contained unique sublime collections of information, the board sub-systems, making an increasingly careful definition deceiving [4].

10.1.2.1 EHR technical issues

A typical EHR or of its collaboration's with other social protection structures that can decrease care quality or patient outcomes. Other social protection systems fuse individuals, care gatherings, workplaces, courses of action, care strategies, and human administrations affiliations. Imperfections may be displayed in the midst of the assurance, structure, plan, or perpetual improvement times of the EHR lifecycle.

10.1.2.2 EHR characteristics

In association with medicinal services to enhance and enlarge the utilization of EHR clearly intended for Certified Commission of Health Care Report, Computerized Maintenance and Management System, and other human service agencies.

10.1.2.3 Mandatory safety for EHR in an organization

- Care-process change (thoroughgoing upgrade of medicinal services procedures to accomplish critical enhancements in clinical results, benefit levels, and expenses).

- Persistent wellbeing (reliable, association-wide endeavors to enhance quality with long-suffering results).
- Client-support building (appropriate advances to hierarchical, group, or individual requirements).
- Programming wellbeing (utilization through frameworks building strategies to lessening the dangers related to programming plan and utilization).
- Task the board (the utilization of express administration practice to the venture to augment benefits and limit expenses, counting dangers).
- Persistent enhancement (constant, methodical endeavors to enhance procedures and results).

10.2 Terminologies

10.2.1 *Safety and effectiveness of EHR*

Looking over the general security and reasonability of EHR use is made inconvenient by the compelled research composing. A couple of available examinations have, as it were, been coordinated by the architects of the EHRs and have focused on the effect of solicitation entry (CPOE) structures on a foreordained number of slip-up sorts [9,10]. Although a couple of extents of error showed improvement, all things considered, security and sufficiency have been tended to in only five examinations [11,12]. Although the underlying two examinations have been comprehensively referred to as showing Computerized Physician Order Entry (CPOE) benefits, neither exhibited overhauls in patient outcomes [10,13]. In all honesty, the second examination uncovered an extension in prescription oversights and hostile drug events, which was turned around after an upgrade in the CPOE interface [13]. The third examination, coordinated in a subpopulation of a children's specialist's office, documented a duplicating of mortality (from 2.8% to 6.6%) after Computerized Physician Order Entry use [14]. The fourth examination, drove in a comparative specialist's office, showed no colossal change in mortality [15]. The fifth examination found that only 31% of specialists and 56% percent of therapeutic overseers believed that the EHR added to improvement of thought speaking by and large [12].

In a systematic review of robotized clinical-decision help, Garg *et al.* contemplated that "only seven primers uncovered upgraded patient outcomes ... and no examination declared favorable circumstances for huge outcomes, for instance, mortality. Surrogate patient outcomes, for instance, circulatory strain and glycated hemoglobin, were not really improved in numerous examinations" [16]. A later exact review of human administrations information advancement (all things considered, EHRs) by Chaudhry *et al.* contemplated that in most human administrations settings, it may be problematic "to make sense of what points of interest to envision from prosperity information advancement use and how best to execute the system with the true objective to expand the regard inferred" [17]. A proficient study of outpatient Computerized Physician Order Entry structures found only four examinations that kept an eye on security and wrapped up "the reasonably unobtrusive number of evaluation considers disseminated to date don't give adequate

verification that Computerized Physician Order Entry structures overhaul prosperity and diminishing expense in the outpatient settings” [18]. Another deliberate review of the effect of EHR use on the idea of outpatient care achieved a likewise negative resolution [19].

Past the dispersed composition, what is the confirmation that EHRs can reinforce as a rule improvement in patient security? On basic source of confirmation is the experience of affiliations that usage for the most part create EHRs [1]. In those affiliations, including those of the makers, clinicians regard straightforward access to test outcomes, clinician recognitions, clinical-decision help, and e-educating as essential to mind quality and patient prosperity. Understanding security programs, for instance, tranquilize bargain at the advances between the outpatient and inpatient settings, depend essentially on the EHR to make them conceivable and effective.

10.2.2 Safety imperfections in EHR

Entangling matters, the human services writing reports the capability of EHRs to add to wellbeing episodes and patient mischief [1,14,20,21]. Beyond these distributed reports, a few associations have by and large distinguished and archived a great many possible EHR-needed security blemishes [22]. All these imperfections were recognized and alleviated previous to a wellbeing occurrence happens.

The reports of patient devilishness state all the additionally with respect to the dangers of hazardous EHR utilization than they do about EHRs as such [23,24]. But to the degree this is legitimate, it essentially raises additional issues: What are the positive and negative effects of EHRs as executed on thought quality, including security? What execution components are connected with those positive and negative effects? What EHR structure, use, and relentless improvement practices will incite increased productive results and restricted negative effects? These requests ought to be answered as fast as considering the present situation.

10.2.3 EHR safety steps

Without distributed research that distinguishes an exhaustive arrangement of compelling danger decrease exercises, medicinal services associations (huge and little), EHR merchants, and EHR assessors require a break, businesslike structure for guaranteeing EHR security. This structure needs to consider the full EHR lifecycle, including plan, usage in an explicit association, and constant enhancement after execution. We propose seven stages that human services associations, EHR sellers, and assessor could attempt to show the guarantee of security enhances even as selection turns out to be increasingly across the board.

10.2.4 Using EHR as a tool in health care process

Social insurance associations should approach EHR execution and constant enhancement as a major aspect of their general procedure enhancement endeavors. This methodology will strengthen the way that sheltered and viable utilization of an EHR requires new hierarchical arrangements, forms, work frameworks, sets of

expectations, and training [25,26]. This should begin with the express acknowledgment of wellbeing as an essential objective of all buying, execution, and persistent enhancement endeavors. This would require clinical tasks pioneers, human services informaticians, and frameworks security specialists to apply their consolidated hypothetical and functional learning to every one of the phases of the EHR lifecycle. It may incorporate assigning an EHR wellbeing officer who reports to the Chief Medical Information Officer or Chief Quality Officer. Little healing facilities and most doctor rehearses are probably not going to have the assets to mount such an activity. They will require access to reasonable, safe EHRs that require at least nearby adjustment and testing—what Greenhalgh *et al.* allude to as an “increased item” that incorporates care-process upgrade proposals, usage and nonstop enhancement benefits, an assistance work area, and specialized help [27].

EHR merchants ought to determine and plan their items to help elite procedures and proceeding with process upgrade. Human services assessors, payers, and approach creators should outline their drives and commands from this equivalent point of view. For instance, requiring and paying for enhanced human services procedures and results (that are not practical without the successful utilization of an EHR) is probably going to be more gainful than paying for the execution of EHRs as such. At last, scientists ought to create hypothetical and down to earth learning in regards to the most secure and best approaches to utilize EHRs to help enhanced consideration forms. For instance, the present limited spotlight on request passage (CPOE) ought to be widened to address the iterative, interdisciplinary procedure of request the executives that doctors, drug specialists, medical attendants, and others take an interest in.

10.3 Medical record maintenance

10.3.1 Implementation and design of safe EHR

Social insurance associations ought to comprehend their EHR-related security needs and expect sellers to address those necessities. At its most fundamental, this implies asking what programming security faculty and practices the seller employments. Bigger medicinal services associations should create counseling connections or in-house assets in programming wellbeing and human variables building to direct EHR obtaining, usage, and consistent enhancement [28,29]. Smaller associations will require access to increased EHRs and to fair, significant data on the security qualities of explicit items and execution choices.

EHR sellers should make security an essential objective from the most punctual phases of detail and structure. Techniques created in different ventures should be adjusted to social insurance [28]. The Certification Commission for Healthcare Information Technology (CCHIT; <http://cchit1.webexone.com>) taught to interpret programming security standards and practices into criteria for accreditation [28]. Leapfrog (<http://www.leapfroggroup.org/>) and different

business alliances should make great programming wellbeing rehearses a basis for interest in their projects.

10.3.2 Achieving performance in EHR using safety testing and reporting mechanism

As the intensity of EHRs to impact care choices is progressively perceived and EHRs are utilized to robotize expanding quantities of consideration forms, early proposals for intentional, nearby oversight of EHR security [30] are probably going to be supplanted by prerequisites (maybe implemented by the U.S. Nourishment and Drug Administration) that EHR sellers and medicinal services associations test and report freely on the wellbeing of their product frameworks. Ahead of time of this, social insurance associations ought to assess the wellbeing of their EHRs deliberately and report their security systems, examinations, and results. Merchants ought to depict their wellbeing testing programs and any security imperfections they (or one of their clients) find to the majority of their clients. Jump has made an essential preliminary stride by building up a framework for testing the wellbeing and viability of executed request section frameworks [31].

In this specific situation, it is vital to recollect that testing is just a single part (and maybe the minimum successful part) of a product security program. Programming wellbeing includes distinguishing potential framework defects to be controlled and arranging how to control them as the framework is being indicated and configuration starts. Changing a product framework as perplexing as an EHR after it has been created (or actualized) is hugely troublesome, mistake inclined, and costly. Consequently—and significantly more vitally for patient wellbeing—proactive security endeavors must be accentuated over responses to wellbeing defects or episodes found in the field [28].

A counseling organization, KLAS (<http://www.healthcomputing.com/Klas/Site/>), studies many human services associations on their encounters with explicit programming items consistently. Associations directing EHR wellbeing reviews, for example, KLAS, should add addresses, for example, these to their overview: “Does the seller tell you proactively of EHR-related security blemishes and suggest hazard relief techniques?” and “Does the merchant react expeditiously when you recognize a potential EHR-related security defect?” Finally, specialists should think about how EHRs can be tried in manners that are both educational and asset productive.

10.3.3 Managing and preventing EHR-related flaws

Nearby EHR execution and consistent enhancement groups settle on numerous choices—with respect to authoritative arrangements, work procedures, and programming setups—that can possibly make framework security blemishes. In the event that it distinguishes a potential defect, an association ought to advise its EHR merchant, who might have the capacity to give a product upgrade that evacuates the blemish. In the event that the imperfection cannot be evacuated by changing the product, the association may need to change a procedure or approach. In the event

that this is unimaginable, the association should expel the capacity from the EHR. In the event that isn't practical, clients must be cautioned amid preparing (and now and again more than once after go-live). Associations should follow their endeavors to relieve each imperfection and any wellbeing occurrences that happen.

The distinguishing proof of EHR-related imperfections increments notably with each new programming sending (both unique usage and updates) [13,32]. This makes plentiful quantities of "shadow coaches" (who watch EHR clients, answer questions, give without a moment to spare instruction, and report blemishes to the war room) a need [27]. A 24×7 medical emergency that filters for blemishes and episodes, makes fast fixes, and imparts them to clients is additionally fundamental. This help group ought to distill exercises learned into new (or refined) techniques for future programming structure, arrangement, testing, and preparing [33].

A second fast reaction group is expected to oversee EHR-related security occurrences. This group ought to incorporate pioneers of clinical activities, the EHR bolster group, informatics, data security, quiet wellbeing, hazard the board, and advertising. The group must be equipped for meeting on a couple of hours' notice to plan and complete restorative activity. All EHR clients who may experience the defect that prompted the occurrence must be cautioned of the blemish while the fast reaction group at the same time guarantees that the imperfection is expelled from the framework and plans any fundamental patient correspondences and other healing activities. Little associations should scale their quick reaction group to the accessible assets. This need will give another impetus to little associations to buy in to an enlarged EHR item that gives occurrence the executives bolster or to join an EHR agreeable. Between hierarchical tolerant prosperity community situated should help affiliations huge and little by adding EHR security to their plans [34].

10.4 Medical data breach

An investigation of information ruptures answered to the California state lawyer general's office in 2012 found that the human services division was third in the quantity of information breaks, after the retail segment and fund and protection area. What's more, in spite of the fact that the information ruptures in the medicinal services industry so far have come about essentially from coincidental breaches, for example, the passing of a PC or cell phone, some security experts caution that the individual data in the records are viewed as progressively significant for character hoodlums and others.

Medicinal records order a lot higher underground market cost than charge card numbers, which is the reason Rick Kam, leader of the information security counseling firm ID Experts in Portland, Oregon, anticipates fraudsters giving careful consideration to restorative data than they have before.

The issues fall into two general classifications, the product itself and human inability to receive great practices.

Numerous examinations have discovered extremely fundamental vulnerabilities in EHR programming, said Laurie Williams, PhD, a software engineering teacher at North Carolina State University. Her exploration group's examination of a couple of EHR frameworks discovered they were available to "nearly tenderfoot dimension security assaults."

Poor security is an endemic issue with programming in numerous businesses, and "the product itself is most likely no more regrettable than in different areas," Williams said. Numerous different sorts of programming contain comparative vulnerabilities, yet the EHR issues are upsetting in light of the fact that they contain such touchy and individual data. Williams said that if a programmer acquires Mastercard data, a client can fix the harm by shutting the record and getting another charge card, "yet with wellbeing records, if somebody's private data gets out, you cannot pull back that learning."

Potential issues run from fraud from the arrival of data, for example, Social Security numbers to malignant messing with records themselves. "You could change somebody's blood classification and afterward they'd get a transfusion of the wrong sort," Williams said.

Rubin noticed that casualties of data fraud can have cash stolen and their credit destroyed, however medicinal exposures present exceptional perils. "There are a ton of dangers to individuals having their medicinal information uncovered," he said. There is a hazard about not having the capacity to land a position in light of the fact that [you] have a specific hereditary cosmetics, or simply disgrace from having certain sicknesses."

10.5 Technical issues

At the point when noteworthy security imperfections or occurrences are recognized, various EHR partners require fast notice. Proficient social orders (for example, the Association of Medical Directors of Information Systems) and EHR clients' gatherings have as of late started utilizing email list-fills in as casual warning frameworks. Sellers are additionally starting to advise their clients of imperfections (alongside arrangements). To make these frameworks maximally viable, associations that utilization EHRs ought to tell their merchants speedily of the blemishes they recognize. A portion of these defects will end up being identified with the seller's product creation process; others will have been presented by the client or by communications between the EHR and other social insurance frameworks. Frequently, this qualification will be hard to make. Regardless, sellers should scan for different occurrences of the imperfection and prescribe to their different clients suitable programming redesigns or setup changes. (Notwithstanding when blemishes are made by nearby setups or communications between neighborhood EHRs and different frameworks, the seller will regularly have the capacity to make the best arrangement by overhauling the EHR programming over its distinctive modules, for instance, inpatient, outpatient, and drug store on account of prescription compromise.)

EHR clients and sellers ought to likewise present the defects and occurrences they distinguish the nationwide cleaning houses. Were this cleaning houses ought to an overseen to believed association, structured with the goal that every association can audit the information it submits and in addition seeing every one of the information from its merchants' clients and the whole clearinghouse in anonym zed frame. Merchants ought to have the capacity to see the information put together by their clients and the entire database—both in anonym zed shape. Specialists ought to approach the total, anonym zed database. This database would give these partners basic data of the scope for EHR-needed blemishes its episodes and further updates of an event. Patients, controllers, decision makers, etc. should investigate strategies for securing members' privacy and giving motivators to interest.

The clearinghouse ought to be founded on a very much planned scientific categorization of EHR-related framework wellbeing blemishes and security episodes, which still cannot seem to be produced. Distributed reports of CPOE-related mistakes have given beginning, abnormal state typologies of security episodes [20,35,36]. However, their attention on request passage is a considerable confinement, since imperfections and occurrences are not restricted to the request section period of consideration [37]. Indeed, where various EHR parts are incorporated (for instance, arrange section, nursing and drug store arrange handling, and medicine organization documentation), a standout amongst the most imperative wellsprings of needed of EHR blemishes to be associations amid segments. What's additional, the distributed structure is tended to such basic issues as the impact of the dimension of clinical-choice help robotization on security imperfections and their probability of adding to a wellbeing episode [28,38].

10.5.1 Storing and preserving the storage of records for long pursuit

Capacity that apply standard and interoperable answers to oversee and save electronic wellbeing records (e.g., lab test results, CT checks, doctor notes, and so on) as well as move, appropriate, duplicate, and access these records from heritage arrangements and stages to cutting edge standard designs and working frameworks are indispensable for clinical consideration and medicinal research. Be that as it may, the board and interoperability for conservation, stockpiling, and availability of such wellbeing information has not yet been characterized for electronic wellbeing records (EHR).

10.5.1.1 NIST approach

Through research and in addition joint effort with government, standard advancement associations, and industry, NIST scientists are attempting to make a standard protection framework to help a wide assortment of electronic wellbeing records, information organizations, and conveyance systems and also distinguish, assess, and coordinate standard and best practice long haul conservation and the executives devices to move, recreate, and circulate EHRs. This activity will empower NIST specialists to actualize an all-inclusive informing mapper to parse a broad scope of

conventions, store clinical learning into an all-inclusive archetype-based record configuration, and seek, recover, and get to put away electronic wellbeing records in the long haul. The figures underneath demonstrate by and large utilitarian outline and give the framework design.

10.5.2 *Synchronization of records*

Synchronization suggests invigorating two or a couple of data sources, where a data source is either a database or a flexible contraption (Personal Digital Assistance, Mobile, etc.) [39]. Seeing as enormous excitement for zone data communicate and harmonization, obviously lots of usages were delivered. Studies have been finished in order to depict and regulate synchronization frames. Due to this standardization methodology the principle variation of the Synchronization Markup Language set [33] was exhibited in 2000 by a consortium of associations. This standard hopes to formalize the various types of synchronization process and to give XML detail to unequivocal depiction of exchanged messages. It is an open standard, making it possible to incorporate new limits, for instance, those required for data security. Synchronization Markup Language [33] portrays two classes of synchronization: single direction synchronization and two-way synchronization.

In a confined synchronization process, a singular data source sends data to various targets. The goals store the got data anyway never send data back. The client or the server may go about as the wellspring of the data stream. In case the source is the client, the sorts of synchronization are: one-course change from client (the source is the client and the server joins the new data with existing data), fortify coordinate from client simply (like the past case yet with the server replacing the present data by the new data). If the source is the server there is: one-way coordinate from server (the source is the server and the client merges the new data with the present data), resuscitate synchronize from server simply (similar, anyway with the client overriding the present data by the new data), and server alert (the server sends a caution to the client).

In a two-way synchronization procedure, server and client then again expect the activity of source and target. There are two such sorts of synchronization: two-way modification (the client begins by sending changes since the last synchronization; the server merges the data, sends its modifications back in conclusion the client joins the data) and moderate coordination (the client sends its absolute enlightening list, by then the server examinations the data field-by-field and returns the adjustments back to the client).

The Synchronization Markup Language movement is by and by joined past any binding impact Mobile Alliance (OMA), made out of around 200 associations including the world's driving versatile managers, device and framework suppliers, information advancement associations, and substance and authority communities [29].

In the helpful territory, everyone is concerned by the idea of thought. Not withstanding whether we are patients, people from the helpful staff, medicate authorities or back up plans, we by and large undertaking to expand the extent among

time and nature of thought or cost and nature of thought. A lot is on the line around there and various associations have begun to make things passing on an all out course of action, for example changed in accordance with each on-screen character related with the restorative administrations process. The tremendous number of answers returned from an output for “EHR” using MEDLINE database or a web crawler (Google, MSN, etc.) shows the significance of this issue.

Diverse therapeutic foundations are captivated by data synchronization not solely to ensure EHR data exchange yet notwithstanding grant transportability and cooperation for their staff [9,40]. Data synchronization shapes between mending focus information structures and PDAs have been considered by Campana [41], who separated XML-based synchronization of patient records between a PDA and a central data server. Unfortunately, his approach does not cover our awesome setting with various synchronous clients and a propelled access rights the officials.

Synchronization considering the data stream between a couple of clients and one server, we are surely in a two-way synchronization show, since the server must send to a client the data as of late made by various clients. Rights the board with the true objective that the client doesn’t think about the entire enlightening accumulation and it is the server’s business to understand the changes. Our system in this way resembles the standard moderate coordinate strategy.

Management among the customer and member of staff serving at table pursues following stages:

1. The client instates procedure for a patient and customer readies the information and approaches the server for a “go/no-go” reaction.
2. The attendant check approvals, confirms whether synchronization is required lastly checks for conceivable clashes.
3. The customer sends the information trees.
4. The server appoints new IDs to trees and hubs and stores them. These IDs, called aggregate IDs, are the IDs in the aggregate database and exceptionally distinguish the information in the system. The server sends to the customer both the aggregate IDs (through mapping tables: neighborhood IDs and aggregate IDs) and the information put away by different customers on the server since the last synchronization of this customer. We should see that just the information that the client is approved to see are sent to the customer, as indicated by our rights the executives rules.
5. Finally, the customer refreshes its neighborhood database, supplanting nearby IDs with aggregate ones and putting away the new trees.

Creating New User in EHR

```
<tree id="1" >
<node id="1" text="name"/>
<node id="2" text="Jean"/>
</tree> and he needs to include the location of the patient; the tree progresses
toward becoming:
<tree id=1>
```

```

<node id="1" text="name"/>
<node id="2" text="Jean"/>
<node id="i" text="address"/>
<node id="ii" text="15 First Street"/>
</tree>

```

10.5.3 Customization of HER

The medicinal services world keeps on changing just before our eyes, with steady innovation upgrades thus enhancing social insurance strategies and conveyance for billions of patients. The advancement of EMR has done a lot to enhance the social insurance encounter, yet this is certainly not an opportunity to get self-satisfied. EHR formats keep on developing, going up against highlights that make them increasingly effective, progressively exact, and far simpler to utilize. In this time of consistently changing EMR layouts, it could really compare to ever for practices to consider a lot of EMR format customization. Unyielding EMR layouts can without much of a stretch draw a generally suitable practice under. Here are the reasons as follows.

10.5.3.1 Efficiency

Therapeutic experts frequently whine about EHR formats, and in light of current circumstances, the conventional EHR layouts happen to be very unbendable. With such formats, specialists, medical attendants, and authorities are compelled to address patients in words that are not their own and could possibly apply straightforwardly to the current circumstance. In the meantime, layouts can accommodate astonishing productivity, a quality that is undoubtedly required in the harried therapeutic world.

The primary preferred standpoint of EHR layout customization is that it gives productivity without straitjacketing the medicinal expert into a content that sounds totally unnatural and ill suited for the job needing to be done.

10.5.3.2 Personalization

As referenced above, standard EMR formats are restricted in that the location all patients as though they are one and the equivalent. The truth of the matter is, each patient's conditions might be only somewhat unique, and, in the event that you cannot address these distinctions, you could be doing your patient an immense injury.

EMR format customization enables you to modify layouts to such an extent or as meager as required dependent on the patient's exceptional circumstance. You'll feel better realizing that you have done your best to furnish all patients with incredible medicinal medications and far better bedside habits.

10.5.3.3 Organization of data

Now, featuring the advantages of electronic wellbeing records over the conventional paper technique ought not be fundamental. In any case, you'd be astounded at what number of medicinal experts keep on terrible talk EMR formats while

overlooking the numerous issues that went with past strategies for electronic wellbeing records.

Layouts have served the medicinal foundation well throughout the years in that they offer unparalleled association capacities. Printed material is far less inclined to be lost when it is accurately put away and always available through the progressed EMR framework. EHR layout customization takes the upsides of EMR to an unheard of level by tending to a considerable lot of the normal worries that kept therapeutic experts from going up against the electronic arrangement in any case.

10.5.3.4 Emergency

While medicinal crises are standard for practices and particularly in crisis rooms, a few crises go up against an unexpected scale in comparison to other people. At the point when a crisis happens on an enormous scale, it is critical for restorative foundations have the capacity to address the circumstance rapidly and productively.

For instance, when a medication review happens, rehearses must contact patients recommended the medication being referred to, give potential substitutions, and address any potential issues that may have happened because of taking that sedate. EMR layout customization can give therapeutic practices the instruments they have to deal with such a mass scale activity.

EMR format customization has turned into the methodology of decision for therapeutic experts everywhere throughout the world. Abandon straitjacketed feeling of conventional EHR formats and bamboozle the two universes with EHR layout customization!

10.6 eHealth and teratology

The sharing of patient data between medicinal services associations and IT frameworks is transforming from a “point to guide” display toward a “numerous to many” one. The European Commission is supporting moves to encourage cross-outskirt interoperability of e-wellbeing frameworks and to evacuate potential lawful obstacles, as in the task www.epsos.eu/. To take into account worldwide shared work process, studies will be bolted when they are being perused and after that opened and refreshed once perusing is finished. Radiologists will have the capacity to serve different social insurance offices and read and report crosswise over extensive topographical territories, hence adjusting outstanding tasks at hand. The greatest difficulties will identify with interoperability and legitimate clearness. In a few nations it is nearly illegal to rehearse teleradiology. The assortment of dialects talked is an issue and multilingual detailing formats for every single anatomical district are not yet accessible. Be that as it may, the market for e-wellbeing and teleradiology is advancing more quickly than any laws or directions.

10.7 Building a safety EHR safety metrics

Medicinal services associations should report their arrangements and methodology (counting testing and imperfection following) for guaranteeing EHR security and

survey them yearly. Assessors, for example, the Joint Commission should screen consistence. EHR merchants ought to incorporate EHR wellbeing best practices in their execution preparing and documentation. Clients' gatherings ought to give data on advancing EHR security best practices.

A critical subsequent stage in enhancing EHR wellbeing will be to assemble specialists from clinical practice, clinical activities, informatics, human elements designing, data innovation, and patient security to make accord on what is at present thought about guaranteeing EHR wellbeing. Human elements specialists and teachers should then lead the advancement of usable apparatuses that empower social insurance associations and EHR merchants to pursue those accepted procedures routinely. At long last, orderly investigation into the forecast, counteractive action, and the board of EHR-related security defects and episodes is expected to make the information base on which enhanced medicinal services procedures and EHRs can be constructed.

10.8 Conclusion

Learning of how to create, execute, and ceaselessly enhance EHRs for patient wellbeing is as of now constrained and not open to most human services associations. Social insurance associations, EHR merchants and assessors, medicinal services informaticians, security engineers, human components engineers, and different partners must sort out and spread what is right now known and make a revealing framework that will propel comprehension of EHR-related wellbeing blemishes. They should cooperate to progress EHR wellbeing learning and practices with the goal that no patient is hurt by an EHR.

References

- [1] McDonald C. Computerization can create safety hazards. *Ann Int Med* 2006;144:510–516.
- [2] Brown M, Grimm N, and Shaw N. The relationship between electronic health records and patient safety: a joint report on future directions for Canada. Toronto, ON: Canada Health Infoway; 2007. pp. 1–31.
- [3] Kohn L, Corrigan J, and Donaldson M. *To Err Is Human: Building a Safer Health System*. Washington, DC: National Academy Press; 1999.
- [4] Tang P. Safety CoDSfP: key capabilities of an EHR system. Institute of Medicine. Washington, DC: National Academies Press; 2003. pp. 19.
- [5] Carayon P, and Karsh B. Sociotechnical issues in the implementation of imaging technology. *Behav Inform Technol* 2000;19:247–262.
- [6] Eason K. Understanding the organizational ramifications of implementing information technology systems. In: Helander M, Landauer T, Prabhu P, editors. *Handbook of Human-Computer Interaction*. New York, NY: Elsevier Science; 1997. pp. 1475–1495.

- [7] Eason K. Changing perspectives on the organizational consequences of information technology. *Behav Inform Technol* 2001;20:323–328.
- [8] Karsh B. An examination of employee participation during new technology implementation. *Journal of the American Medical Informatics Association*, 1997;41(2):767–771.
- [9] Kaushal R, and Bates D. Computerized physician order entry (CPOE with clinical decision support systems [CDSSs]). Evidence Report/Technology Assessment No. 43. In: Wachter R, editor. *Making Health Care Safer: A Critical Analysis of Patient Safety Practices*. Rockville, MD: Agency for Healthcare Research and Quality; 2001.
- [10] Berger R, and Kichak J. Computerized physician order entry: helpful or harmful? *J Am Med Inform Assoc* 2004;11:100–103.
- [11] Bates DW, Leape LL, Cullen DJ, *et al*. Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. *JAMA* 1998;280:1311–1316.
- [12] Weiner M, Gress T, Thiemann DR, *et al*. Contrasting views of physicians and nurses about an inpatient computer-based provider order-entry system. *J Am Med Inform Assoc* 1999;6:234.
- [13] Bates DW, Teich JM, Lee J, *et al*. The impact of computerized physician order entry on medication error prevention. *J Am Med Inform Assoc* 1999;6:313–321.
- [14] Han YY, Carcillo JA, Venkataraman ST, *et al*. Unexpected increased mortality after implementation of a commercially sold CPOE system. *Pediatrics* 2005;116:1506–1512.
- [15] Del-Beccaro M, Jeffries H, and Eisenberg M. Computerized provider order entry implementation: no association with increased mortality rates in an intensive care unit. *Pediatrics* 2006;118:290–295.
- [16] Garg AX, Adhikari NKJ, McDonald H, *et al*. Effects of computerized clinical decision support systems on practitioner performance and patient outcomes. *JAMA* 2005;293:1223–1238.
- [17] Chaudhry B, Wang J, Wu S, *et al*. Impact of HIT on quality, efficiency, and costs of medical care. *Ann Int Med* 2006;144:E-12–E-22.
- [18] Eslami S, Abu-Hanna A, and deKeizer N. Evaluation of outpatient computerized physician medication order entry systems: a systematic review. *J Am Med Inform Assoc* 2007;14:400–406.
- [19] Linder JA, Ma J, Bates DW, Middleton B, and Stafford RS. Electronic health record use and the quality of ambulatory care in the United States. *Arch Intern Med* 2007;167:1400–1405.
- [20] McNutt R, Abrams R, and Aron D. Patient safety efforts should focus on medical errors. *JAMA* 2002;287:1997–2001.
- [21] Horsky J, Kaufman DR, Oppenheim MI, and Patel VL. A framework for analyzing the cognitive complexity of computer-assisted clinical ordering. *J Biomed Inform* 2003;36:4–22.
- [22] Campbell E, and Sittig D. Types of unintended consequences related to computerized provider order entry. *J Am Med Inform Assoc* 2006;13: 547–556.

- [23] Longhurst C, Sharek P, Hahn J, Sullivan J, and Classen D. Perceived increase in mortality after process and policy changes implemented with computerized physician order entry. *Pediatrics* 2006;117:1450–1451.
- [24] Sittig D, Ash J, Zhang J, Osheroff J, and Shabot M. Lessons from “Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system.” *Pediatrics* 2006;118:797–801.
- [25] Carayon P, Hundt AS, Karsh B-T, *et al.* Work system design for patient safety: the SEIPS model. *Qual Saf Health Care* 2006;15(Suppl 1):50–58.
- [26] Karsh B-T. Beyond usability: designing effective technology implementation systems to promote patient safety. *Qual Saf Health Care* 2004;13:388–394.
- [27] Greenhalgh T, Robert G, Macfarlane F, Bate P, and Kyriakidou O. Diffusion of innovations in service organizations: systematic review and recommendations. *Millbank Q* 2004;82:581–629.
- [28] Leveson N. *Safeware: System Safety and Computers*. Reading, MA: Addison-Wesley; 1995.
- [29] Kleiner B. Sociotechnical system design in health care. In: Carayon P, editor. *Handbook of Human Factors and Ergonomics in Health Care and Patient Safety*. Mahwah, NJ: Lawrence Erlbaum; 2007.
- [30] Miller RA, and Gardner RM. Summary recommendations for responsible monitoring and regulation of clinical software systems. *Ann Intern Med* 1997;127:842.
- [31] Kilbridge P, Welebob E, and Classen D. Development of the Leapfrog methodology for evaluating hospital implemented inpatient computerized physician order entry systems. *Qual Saf Health Care* 2006;15:81–84.
- [32] Shulman R, Singer M, Goldstone J, and Bellingan G. Medication errors: a prospective cohort study of hand-written and computerised physician order entry in the intensive care unit. *Crit Care* 2005;9:R516–R521.
- [33] Walker JM, Richards F, and Bieber E. *Implementing an Electronic Health Record System*. New York: Springer; 2005.
- [34] Carayon P, Kosseff A, Borgsdorf A, and Jacobsen K. Collaborative initiatives for patient safety. In: Carayon P, editor. *Handbook of Human Factors and Ergonomics in Health Care and Patient Safety*. Hillsdale, NJ: Lawrence Erlbaum; 2007.
- [35] Ash JS, Sittig DF, Dykstrab RH, Guapponea K, Carpenterc JD, and Seshadria V. Categorizing the unintended sociotechnical consequences of CPOE. *J Med Inform* 2007;76:S21–S27.
- [36] Ash J, Sittig D, Poon E, Guappone K, Campbell E, and Dykstra R. The extent and importance of unintended consequences related to computerized provider order entry. *J Am Med Inform Assoc* 2007;14:415–423.
- [37] Fortescue EB, Kaushal R, Landrigan CP, *et al.* Prioritizing strategies for preventing medication errors and adverse drug events in pediatric inpatients. *Pediatrics* 2003;111:722–729.
- [38] Parasuraman R, Sheridan TB, and Wickens CD. A model for types and levels of human interaction with automation. *IEEE Trans Syst Man Cybern Part A Syst Humans* 2000;30:286–297.

- [39] Ash JS, Stavri PZ, and Kuperman GJ. A consensus statement on considerations for a successful CPOE implementation. *J Am Med Inform Assoc* 2003; 10:229–234
- [40] Lehmann C, and Kim G. Computerized provider order entry and patient safety. *Pediatr Clin North Am* 2006;53:1169–1184.
- [41] Kaushal R, Shojania K, and Bates D. Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Arch Intern Med* 2003;163:1409–1416.

Chapter 11

Protection framework and safety standards related to electronic health records

Isabel De la Torre Diez¹ and Aránzazu Berbey-Alvarez²

The traditional clinical history corresponds to the medical record about the treatment received by the patient during the period of his/her illness. The clinical records are legal documents under the principle of confidentiality between doctor and patient. This paper corresponds to a practical application of a secure electronic health record (EHR) system in the cloud at the Vega Baja Hospital in San Bartolomé in Orihuela (Alicante, Spain) taking in account a series of European Directives, recommendations of the European Council of the protection medical data, safety standards in EHRs, and rules of security for healthcare communication. Here, the case study presents an application implemented completely in the cloud.

11.1 Introduction

The clinical history (CH) is a set of documents in the hospital information system that contains personal data, medical value judgments, and observations about the medical situation and evolution of a patient throughout the healthcare process. The CH constitutes the complete record of the care provided to the patient during his/her illness and for this reason, the CH converts in a legal document.

However, its traditional format (paper) entails various difficulties that have become evident during daily medical practice such as: its deterioration or loss, because its paper format can only exist in a place and at a specific time, as well as the presence of an illegible and incomplete medical writing that could make difficult the reading and understanding of the traditional clinical history (TCH).

Another limitation is that TCH can only contribute passively to decision-making because the paper format complicates the patient's medical and scientific analysis.

¹Department of Signal Theory and Communications, and Telematics Engineering, University of Valladolid, Valladolid, Spain

²Vicerrectoría Académica, Universidad Tecnológica de Panamá, Panamá, República de Panamá

The convenience of the electronic health records (EHRs) [1,2] is due that EHRs facilitate and strengthen medical practice in comparison with the traditional CH.

Some of the advantages the EHRs provide are the speed of creation as well as availability and ubiquity, clarity and readability of the data, security, cost reduction, access control, and comfort in the treatment of the patient.

EHR represents a social-technological and management innovation because the HCEs involve incorporating ICT into the core of healthcare activity. As a consequence, CH ceases to be a record of the information generated by the relationship between a patient and a medical professional or a healthcare center and the individual clinical history converts in a part of the integrated clinical information system [3].

All this information that is used in clinical practice must be integrated and stored in a simple and successful way. The management of all medical data duly provides security and confidentiality guarantees.

The development of EHR is largely limited by the requirements and budgets of health centers and available technologies. Therefore, these systems are developed using different concepts that depend on these limitations. These differences can be found between the different EHR systems [4,5].

Telemedicine apps and services often imply many institutions using several technologies and systems. Some European and international institutions are involved in the EHRs standardization. Some of those organizations are the following: European Committee for Standardization Technical Committee (CEN/TC) 251, International Standards Organization Health Informatics Standards Technical Committee (ISO/TC) 215, openEHR, Health Level Seven (HL7), and Integrating Healthcare Enterprise (IHE) [6]. One of the most active in EHRs standards is HL7.

HL7 is used for the exchange of medical information in different specialties. HL7 has been developed by the ANSI organization. In this context, HL7 Clinical Document Architecture (CDA) is another standard based on XML documents, easy to implement and that specifies the structure and semantics of the HCEs. HL7/CDA is used in different medical specialties such as cardiology, ophthalmology, radiology, etc. [7]

Consequently, the adoption of EHRs by the European health system is being quite slow. Most of the previous studies have been carried out in the primary care sector [8], obtaining benefits such as universal access, efficient and efficient coding, among others [9–12].

In great measure, the slow adaptation is due to the difficulty of standardization that the EHRs suppose because there is no concrete model that is satisfied as the most used standard when in fact, there are many examples [13–18]. In the next section, we will try the framework for the protection of personal information. Later, special protection for sensitive data and prohibition of the processing of personal data is shown. In the following sections, we show medical data processing by a professional, safety standards in EHRs, a case study about the implementation of a secure EHRs system in the cloud and in the last section the main conclusion of this chapter.

Table 11.1 General principles of data protection in health

Principle	Definition
Limitation of use	According to Directive—article 6, section 1, letter b: the use of data that is incompatible with the purpose of its collection is prohibited
Quality of the data	Personal data must be not excessive and relevant for the purposes that are collected
Retention	Maximum time to keep personal data should be established
Requirements for information	Those responsible for data processing in EHRs must communicate to the interested party of certain information
Right of access to the interested party	Patients can make sure that their data is up-to-date and verify the accuracy thereof according to article 12 of the Directive
Security obligations	In Article 17 of the Directive, the obligation of the data controller to apply measures (technical and organizational) is defined

11.2 Framework for the protection of personal information in the healthcare context

All treatment of personal data related to health must comply fully with the rules of protection of personal data, respecting the fundamental freedoms and rights of the persons, improving the well-being of persons.

Europe has already taken up the matter with a law governing security and privacy in Health: the European Union Directive on Data Protection 95/46/CE of 1995. It involves a workgroup which unites all of the data protection authorities of the member states and establishes the principles on which all the European Union countries must base their laws.

This group of experts, which initially only met sporadically, has gained in importance and now emits around four reports a year. At the beginning of 2016, the European Union approved a project, the European Data Protection Act. There will be no need to apply this rule in the laws of the member states, given that it will be applied in general. With this new regulation, all the member states will be subject to the same security and data protection: general principles of the protection framework.

The healthcare staff must comply with all the general principles of data protection (shown in Table 11.1).

11.3 Special protection for sensitive data and prohibition of the processing of personal data

The personal data of the patients are extremely sensitive information, therefore it requires special protection. Article 2, letter (a) of Directive 95/46/EC defines personal data as follows:

Personal data” means any information about an identified or identifiable natural person; Any person whose identity can be determined, directly or indirectly, in particular by means of an identification number or one or more

specific elements, characteristic of their physical, physiological, psychological, economic, cultural or social identity, will be considered identifiable.

Article 8 (1) of that Directive defines the special categories of data as follows:

Member States shall prohibit the processing of personal data that reveal racial or ethnic origin, political opinions, religious or philosophical convictions, labor union memberships, as well as the treatment of data relating to health or sexuality.

This definition also applies to personal data when they have a clear and close relationship with the description of a person's health status: data on drug, alcohol or drug consumption, generic data, and all the data that appear in a medical file.

Regarding data protection, taking into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing, as well as the risks of different probabilities and severity of rights and freedoms of natural persons posed by the processing, appropriate technical and organizational measures must be implemented, such as pseudonymization, which are designed to implement data protection principles, integrate the necessary safeguards in the processing to comply with the requirements of this Regulation and protect the rights of the interested parties.

Article 8, paragraph 1, of Directive 95/46/EC on data protection, prohibits the processing of personal data relating to health in general. In this same sense, Article 6 of Convention No. 108 of the Council of Europe does it.

However, taking into account the importance of using information about a patient to treat it medically as it should, there are exceptions to the general prohibition of treatment of medical data. The Data Protection Directive establishes mandatory exceptions in Article 8, paragraphs 2 and 3, which define as follows:

The provisions of paragraph 1 shall not apply in the following cases: when the interested party has given his explicit consent to such treatment, except in cases where the legislation of the Member State provides that prohibition established in paragraph 1 cannot be lifted with the consent of the person.

11.4 Medical data processing by a professional

The impact evaluation of data protection refers to the previous tests and evaluation of effectiveness of the technical, organizational, and procedural configuration. The main objective of the evaluation is to ensure the proper implementation of data privacy, addressing nature and purpose of planned processing operations, questioning how data processing can violate privacy rights and personal liberties, and detailing the risk of exposure mitigation measures and mechanisms.

Article 8, paragraph 3 (D. 95/46/EC) allows to deal out of delicate personal data provided if three cumulative conditions are met. In this way, the treatment of delicate personal data must be necessary, they must be carried out “*for the prevention or for medical diagnosis, the provision of healthcare or medical treatment or the management of health services, and the treatment of the personal data in question must be performed by a health professional subject to professional secrecy or under national law.*”

The exception covers the processing of personal data for an explicit purpose of providing different services related to health of a preventive, diagnostic, or therapeutic nature. Also, for the purposes of the management of these health services, such as billing, accounting or statistics. Subsequent treatment that is not necessary for the direct provision of such service (as medical research, reimbursement of expenses for health insurance, or the filing of pecuniary dues, are not covered).

Other treatments in areas such as public health and social protection are also beyond the scope of Article 8 (3), particularly with regard to quality assurance and cost-effectiveness. As well as the procedures used to resolve claims of benefits and services in the health insurance scheme, given that they are mentioned in recital 34 of the Directive as examples for invoking Article 8 (4).

The processing of personal data contemplated in section 3 of article 8 must be almost necessary for the specific purposes mentioned in letter (a).

According to the Directive, nonmedical staff should not process this sensitive personal data, this staff should also be subject to binding rules that guarantee at least an equivalent level of confidentiality and protection. These rules must contain the obligation that personal information be employed only for the purposes mentioned in Article 8, paragraph 3.

The use of this information is allowed within the limits of the treatment contract. This confidentiality relationship also excludes any third party, including other healthcare professionals, unless the patient has authorized the transmission of their data or this is provided by law particularly.

Regarding the security of the processing, adequate technical and organizational measures must be implemented to guarantee a level of security appropriate to the risk, such as (1) the ability to guarantee the confidentiality, integrity, availability, and continuous resistance of the processing systems and services and (2) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

11.5 Safety standards in EHRs

Table 11.2 shows the security objectives and measures exist to ensure compliance. The two basic security mechanisms are public and private keys, and one-way

Table 11.2 Objective and security measures

Objective	Measures
Identification	Digital certificates
Confidentiality	Encryption
Integrity	Digital signature
Don't repudiate	Digital signature and audit
Authorization	Organizational question that each organization must design and carry out in their particular systems
Audit	Access records and operations carried out on the data
Availability	Operation and level of adequate services on the systems

summary algorithms. These are the foundations for the construction of the rest of security mechanisms.

Thanks to the combining all the objectives and security measures, it is possible to protect information systems through encryption, signature, and digital certificates. The basic and technical mechanisms are complemented with other mechanisms about organization, authorization, audit, operation, and service level.

11.6 **Security for healthcare communication**

A general security framework (CEN ENV 13608-1:2000), security policies have to be established. The instructions about security and data protection include the deployment of public keys, secure certificates, and electronic signature. Data integrity and security are necessary to define safety standards in health. The most important characteristics in CEN TC251 appear in Table 11.3. Other organizations have standards for health safety as ISO with the use of the PKI infrastructure (ISO/CD 17090).

11.7 **Case study: implementation of a secure EHRs system in the cloud**

This case study consists of an offer to support an EHRs application through cloud computing in the hospital environment relatively large in a city. A series of aspects must be considered before considering any solution or implementation. Specifically, the following aspects should be taken into account the following:

- It must be a safe solution.
- Privacy must be provided through efficient authentication.
- Support should be given so that EHRs are accessible by authorized health personnel.
- It must be a robust solution.
- The data can be accessed by a large number of specialists in the same geographical location.
- A large number of health professionals will modify, update or perform some type of operation on the patient's medical history.

Table 11.3 Characteristics in CEN TC251

Characteristic	Function
Strong authentication	It is defined using microprocessor cards for secure user identification (ENV 12251)
Algorithm	It is defined for health digital signature services ENV 12388
Secure user identification	Using passwords for the management of Healthcare and Authentication Security

- It is a health institution with a high level of personnel. The identity is a key factor when developing a secure solution ensuring that only authorized health professionals access the patient's medical history.
- The data must be replicated since we deal with sensitive data this condition will be repeated throughout all application's scenarios. It is vital that there existed a backup of the information against possible fraudulent uses that could cause any losses.
- It must be taken into account that the quality of communications must be acceptable. A fiber service must be available to avoid, as far as possible, the delays caused by communications. We will find some network overload when making simultaneous requests for access to EHRs, so a good network infrastructure will not be able to avoid it altogether, but avoid it in a large extent.
- Each session of access to the data must be secured, in detail, from the access to the data until the closing of the session; it must be secure and never be exposed to possible information fraudulent uses. It is of vital importance in the scenario of the hospital since many physicians will access this data and it is not admissible for there to remain open sessions where there may be "leaks" of information or losses derived from misuse.
- It is taken into account that although there may be large loads of information in motion, the EHRs are largely plain text, although they may sometimes include images of the specialists but it will be based on a supposition of data traffic at a medium level. This will affect the structure of the proposed network and the storage system.

The process will be explained in detail to show the general outline of the solution. Firstly, some aspect to be taken into account before the cloud should be covered. This is necessary because the secure process starts from the same team of the facultative until the end of the communication so that operations before "leaving" the cloud cannot go unnoticed at any time.

11.8 From the optional computer to the cloud

The first essential step is access to the cloud by the doctor or health professional. In the solution, it has been arranged that the data can only be accessed if the medical professional staff is correctly authenticated in the system, otherwise no secure connection can be established with the information system where the electronic clinical records are located.

A schematic view of the second floor of the Vega Baja Hospital in San Bartolomé (Orihuela, Alicante) is shown below in Figure 11.1 [19].

This example has been chosen since the hospital itself is seen very visually, although it is not of the same dimension that La Paz serves as a model to show in a simple way the chosen solution.

Figure 11.2 [20] shows the connection in one of the department (internal medicine). In this case, it is necessary to support an EHR system. As an example, the general scheme would be:

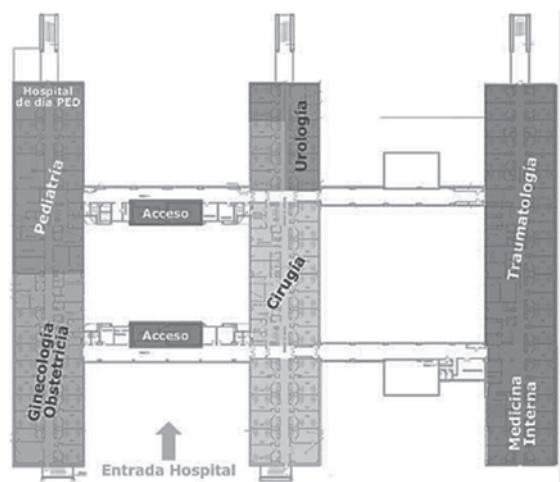


Figure 11.1 *View of the second floor of the Vega Baja hospital in San Bartolomé (Orihuela, Alicante)*

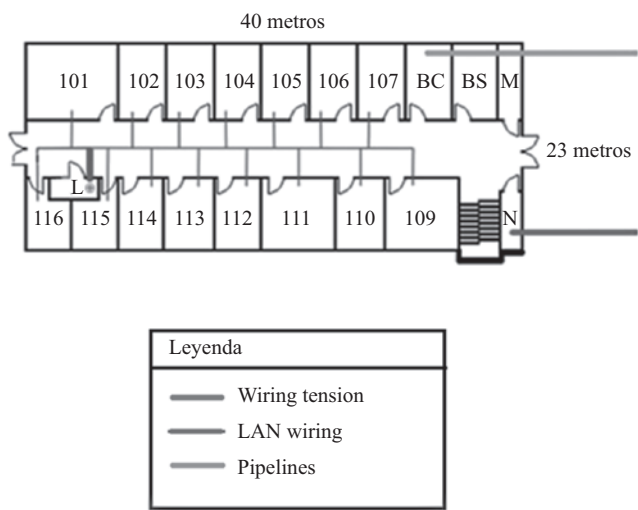


Figure 11.2 *Example of connection of one of the departments of the hospital*

In more detail, we see in Figure 11.3 [20] an example of LAN connection prior to the exit to the cloud. In this image, a hospital department is shown in detail. An environment has been recreated with four consultations of the hospital by way of explanation in detail; this is extendable to all where the installation of these services is required. As shown in Figure 11.3, each department will have its own LAN network, consisting of switches and/or other elements that require in the

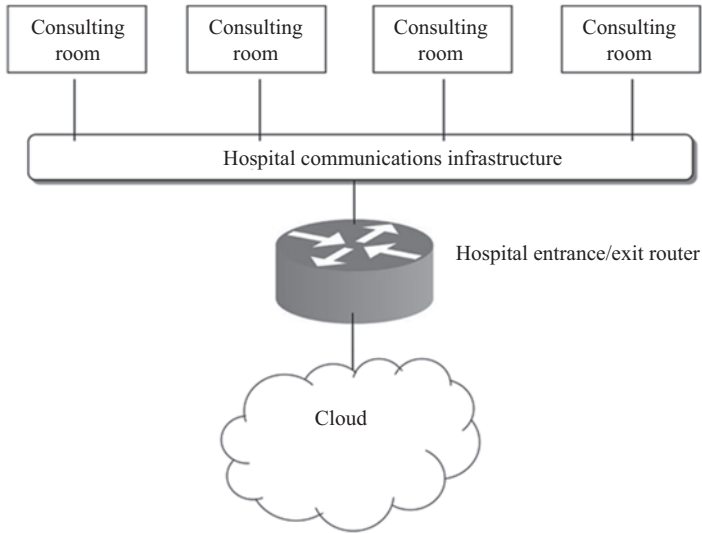


Figure 11.3 Example of the general connection of one of the example departments

department regardless of cloud computing. All these elements locally will be found in any hospital where a system of electronic clinical records is required and will not be specified in detail because it is based on the fact that they will be present as in any common LAN, so its explanation is not necessary. It is expected that in such a scenario the infrastructure will be predisposed for the cloud computing solution.

11.9 Application implemented completely in the cloud

Here, it is presented a secure solution with cloud computing technology and an e-health application fully implemented together with the necessary security and storage elements to provide the service of ECRs in the cloud. Figure 11.4 [20] shows a general scheme.

The application of ECRs is completely implemented in the cloud providing a safe and stable solution. Figure 11.4 shows that the router's output and information input is sufficient for the communication's infrastructure of the hospital. Now the implementation of the cloud for this particular case will be shown when additional information is not necessary. It has been decided to implement before "going out" to the Internet (in the case if the hospital does not already have it) an option of two Cisco ASA fires of the 5500 series [21] with the IP Failover. The reason for this technical decision corresponds to:

- Obtain visibility and granular control of applications and micro applications, with controls based on behavior.
- Robust online security.

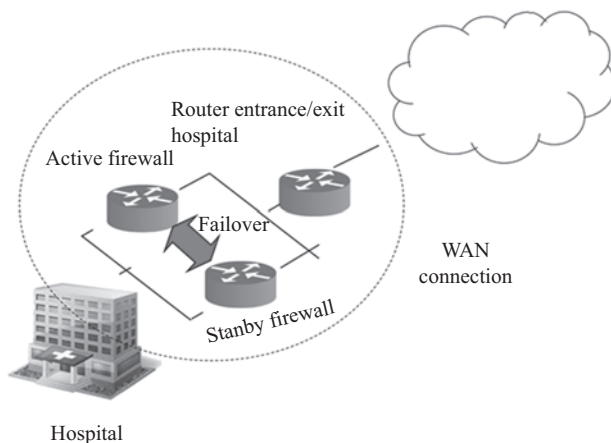


Figure 11.4 General outline of an HCE service implemented completely in the cloud in a hospital

- Protection against threats with intrusion prevention system (IPS).
- Secure remote access.
- Protection against botnets.
- Protection against threats from the Internet.
- Virtual instances that provide security for public and private clouds.

We propose this type of solution about two firewalls working together with the IP Failover configuration. With this configuration, the continuity is achieved in the service. In addition, the load balancing and synchronization between the firewalls is achieved. A 24/7 service is achieved since any hospital cannot allow the service interference, therefore a security solution with confidence to and from the hospital's network is obtained in an uninterrupted manner. We will call this scheme WAN connection onwards so as not to repeat the scheme repetitively.

The cloud internal schema has been decided for this solution is showed in Figure 11.5 [20]. A practical and secure solution has been designed to reach the data from the doctor's query to the database located in the cloud and the application of EHRs can be fully implemented in it.

With the use of two keys, it is possible to protect the storage of accesses without authorization to the data system. Here, the objective is none other can accesses, in the way is possible to protect the confidentiality and integrity of the data, while offering virtual storage.

One of the interoperable key management standards based on the cloud is Key Management Interoperability Protocol (KMIP) from OASIS [22]. It will also cover data encryption and key management for shared storage. It is reflected in Figure 11.5 as a key store.

Once the request has reached the trusted area after passing through the proxy and the agent, the application server will complete the request made about the

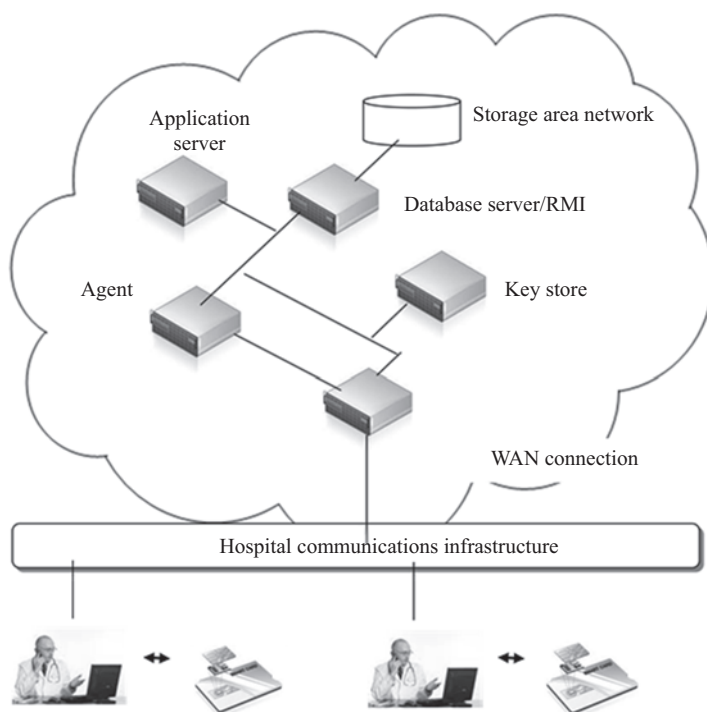


Figure 11.5 Diagram of the infrastructure in the cloud for the complete implementation of HCEs in a hospital

Patient's Clinical History and register it in the database server, which can receive invocations to remote methods on a TCP/IP channel so we get a totally secure and reliable authentication. In addition, it is provided a secure channel confirms that the person trying to access the database is a health professional authorized, therefore once the request is accepted, the application server completes the registration, records the result in the database, and displays it on a Web page on the Web server (in a cloud).

It is proposed as a storage solution as BLOB files (Storage of large binary data), being possible that FILESTREAM storage functionality in them, which allows SQL store large data (BLOBs) directly in an NTFS file system, that is, in any type of hardware that supports it, hard disks, a SAN system, etc., for backup operations, transparently. It is possible to store the data outside the database in a completely transparent way in an NTFS file system. With this functionality, it allows fast access to the information, and frees the server from the database. It is also possible to avoid limiting the databases to a certain capacity because the files and documents are not stored in the database internally. The storage is practically the desired one, which makes it extremely scalable.

In summary, thanks to this type of BLOB files we can have the database, and thus the server in optimal speed and conditions with limited entries, while the data will be stored in a common file system. Therefore in Figure 11.6 shown as BLOB storage is equivalent to database + physical storage in a file system, which will be a storage area network (SAN). This case is not covered because it does not require a detailed explanation, it is proposed to use as many RAIDs 1 + 0 as needed since the storage is practically unlimited with the proposed infrastructure configuration. RAID 1 + 0 has been chosen for data storage because it is just as fast as RAID 0 and also it's tolerable to failures in several disk drives simultaneously; making it an exceptional solution of performance and tolerance to failures. It is the fastest and safest RAID that exists.

The creation of a database of patients will be taken for granted, each with the unique ID that uniquely identifies it, its data, treatments, and all the information that may be necessary for a database. We propose the use of StorageGRID of ByCast. It is virtualization software that can be arranged in the database server, and whose function is created a virtualization layer that gathers storage of different storage devices in a single administration system. Potentially, petabytes of data storage can be collected, different types of storage systems can be used, and protocols can be transported even over dispersed locations geographically.

StorageGRID can manage data from NFS and CIFS file systems over HTTP networks. It is very useful because with NFS and CIFS we can interact with the SAN files systems that will be NTFS to treat the database as BLOB objects. The data can be replicated, migrated to different locations and also retrieved before

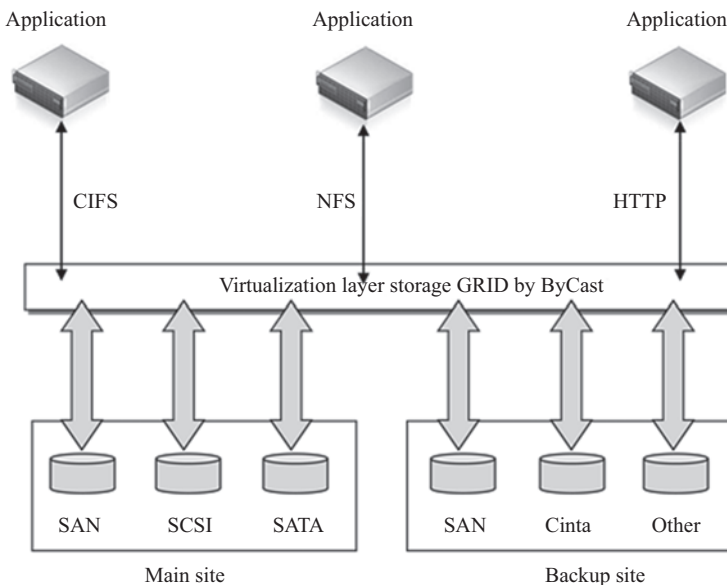


Figure 11.6 Cloud storage system with fault tolerance: StorageGRID of ByCast

failures. The degree of replication is configurable and when storage fails, StorageGRID can be recovered with other copies of the data by redundant systems. With all these features StorageGRID, becomes one of the most important tools within the cloud, because we can virtualize a huge amount of information coming from different physical environments, and also it permits the possibility of recovery from failures, making a very interesting option to take into account by data storage in the cloud time after time.

Figure 11.6 [20] shows the operation of StogareGRID in this case. When it is possible to allow creating a virtualization layer between storage assets and application servers is an important solution to manage cloud storage to prevent any error by tolerant manner.

Thanks to the proposed data storage system through the virtualization layer between the application server and the storage hardware together with the BLOB data system and the RAID 1 + 0 is reached an extremely safe and fast solution to move the information in the cloud and it is displayed on the web server in the most efficient way possible.

11.10 Conclusion

This chapter presents an application implemented completely in the cloud using a case of the Vega Baja hospital in San Bartolomé (Orihuela, Alicante) taking into account the various European rules about Safety Standards in EHRs. The proposed solution uses a Cloud storage system with fault tolerance, StorageGRID of ByCast. The proposal shows that the data storage system permits a safe solution for health information. The main solution is able to move the information in the cloud, displayed on the web server in an efficient way. For that, we propose to use the virtualization layer between the application server and the storage hardware, the BLOB data system and the RAID 1 + 0.

References

- [1] De La Torre-Díez I, Antón-Rodríguez M, and Díaz-Pernas FJ, (June 20th 2011). "Mobile web application development to access to psychiatric electronic health records, telemedicine techniques and applications," In G. Grasczew, and S. Rakowsky (eds.), *IntechOpen*. doi: 10.5772/17148. Available: <https://www.intechopen.com/books/telemedicine-techniques-and-applications/mobile-web-application-development-to-access-to-psychiatric-electronic-health-records>
- [2] De la Torre-Díez F., Barrera-Luengos I., Díaz-Pernas S., *et al.*, "Evolución de e-Health," *Informática y Salud*, vol. 81, pp. 84–90, 2010.
- [3] De la Torre-Díez J.F., Díaz-Pernas I., Antón-Rodríguez F.J., *et al.*, "Requisitos y evolución de los sistemas de e-Health, en," in *Actas de la Conferencia IADIS Ibero Americana WWW/INTERNET 2010 (CIAWI 2010)*, Algarve (Portugal), 2010.

- [4] Ash J.S., and Bates D.W., “Factors and forces affecting EHR system adoption: report of a 2004 ACMI discussion,” *J. Am. Med. Inf.*, vol. 12, no. 1, pp. 8–12, 2005.
- [5] Japan Association of Medical Informatics, “JAMI viewpoint concerning the definition of the electronic medical record,” 2003. [Online]. Available: http://plaza.umin.ac.jp/~jami/publication/denshikarute_en.pdf. [Accessed October 18, 2005].
- [6] Bott O.J., “Electronic health record: standardization and implementation,” in *2nd OpenECG Workshop*, 2004, pp. 57–60.
- [7] Marcheschi P., Mazzarisi A., Dalmiani S., and Benassi A., “HL7 clinical document architecture to share cardiological images and structured data in next generation,” *Comput. Cardiol.*, vol. 31, 2004, pp. 617–620.
- [8] Lo H.G., Newmark L.P., Yoon C., *et al.*, “Electronic health records in specialty care: a time-motion study,” *JAMIA*, vol. 14, no. 4, pp. 609–615, 2007.
- [9] Smith D., and Newell L.M., “A physician’s perspective: deploying the EMR,” *J. Healthc. Inf. Manag.*, vol. 16, pp. 71–79, 2002.
- [10] Kumari A., Tanwar S., Tyagi S., and Kumar N., “Computing for Healthcare 4.0 environment: opportunities and challenges,” *Comput. Electr. Eng.*, vol. 72, pp. 1–13, 2018.
- [11] Vora J., Tanwar S., Tyagi S., Kumar N., and Rodrigues J.P.C., “FAAL: fog computing-based patient monitoring system for ambient assisted living,” in *IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom-2017)*, October 12–15, 2017, pp. 1–6.
- [12] Vora J., Italiya P., Tanwar S., *et al.*, “Ensuring privacy and security in e-health records,” in *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, 2018, pp. 192–196.
- [13] Vora J., Nayyaar A., Tanwar S., *et al.*, “BHEEM: a blockchain-based framework for securing electronic health records,” in *IEEE Global Communications Conference (IEEE GLOBECOM-2018)*, Abu Dhabi, UAE, December 09–13, 2018, no. 1–6.
- [14] Vora J., Devmurari P., Tanwar S., Tyagi S., Kumar N., and Obaidat M.S., “Blind signatures based secured e-healthcare system,” *International Conference on Computer Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France July 11–13, 2018, pp. 177–181.
- [15] Hathaliya J., Tanwar S., Tyagi S., and Neeraj K., “Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach,” *Comput. Electr. Eng.*, vol. 76, 2019, pp. 398–410.
- [16] Tanwar S., Thakkar K., Thakor R., and Singh P.K., “M-Tesla-based security assessment in wireless sensor network, April 07–08, 2018,” in *International Conference on Computational Intelligence and Data Science (ICCIDS 2018)*, 2018.
- [17] Tanwar S., Obaidat M.S., Tyagi S., and Kumar N., “Chapter 10: Online signature-based biometrics recognition,” in M. S. Obaidat *et al.* (eds.),

- Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG, 2019, pp. 255–285.
- [18] Tanwar S., Tyagi S., Kumar N., and Obaidat M.S., “Chapter 21: Ethical, legal, and social implications of biometrics technologies,” In M.S. Obaidat *et al.* (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG, 2019, pp. 535–568.
 - [19] Unidad de Informática del Departamento de Salud de Orihuela, “Plano de la segunda planta del hospital Vega Baja en San Bartolomé (Orihuela, Alicante),” 2019. [Online]. Available: http://www.dep21.san.gva.es/deporihuela/?page_id=293 [Accessed September 20, 2001].
 - [20] Suárez Sanz J., “Estudio de la seguridad y privacidad de soluciones basadas e Cloud Computing en el campo de la e-health,” 2014.
 - [21] CISCO, “Cisco ASA serie 5500,” Firewalls de última generación Cisco ASA serie 5500-X, 2019.
 - [22] OASIS, “Estándar para administración de claves en la nube KMIP de OASIS,” OASIS Key Management Interoperability Protocol (KMIP) TC, 2017. [Online]. Available: <http://www.oasis-open.org/committees/kmip/>. [Accessed September 20, 2001].

This page intentionally left blank

Chapter 12

Security and privacy issues in UK healthcare

*Neetesh Saxena¹, Robin Singh Bhadoria², Sara Dickerson³,
Sophie Branch³, Lucy Dalley³, and Natasha Churchill³*

The healthcare must be a most concern issue for any developed countries in terms of security and wellness of its citizens. In 2015–16, the UK spent £185 billion on healthcare as shown in [1] that provides free medical care to all UK residents, treating 1 million patients every 36 hours as discussed in [2–5]. There must be a governing system which guaranteed the safety, security, and privacy of such data. As such data are vulnerable to cyberattacks and hold the millions of confidential data. This chapter discusses and analyses the various security and privacy issues in the UK healthcare infrastructure and several challenges to be resolved for different attacks.

12.1 Introduction

This section covers the healthcare security and privacy context and the related issues. It also highlights several challenges in resolving the discussed security and privacy issues.

12.1.1 Scope and context

The public healthcare provider in the UK is the National Health Service (NHS) who provides free medical care to all UK residents, treating 1 million patients every 36 hours [5]. An example of a private healthcare provider is the Harley Medical Group who provides cosmetic surgery procedures [6]. Both are vulnerable to cyberattacks as they hold millions of confidential data and have a large financial environment.

12.1.2 Security and privacy issues in healthcare infrastructure

A security issue is a weakness that leaves a company or industry vulnerable to having their confidentiality, integrity, or availability compromised by an attacker

¹Department of Computer Science and Informatics, Cardiff University, UK

²Department of Computer Science and Engineering, Indian Institute of Information Technology (IIIT), Bhopal, India

³Department of Computing and Informatics, Bournemouth University, UK

[7,8]. A privacy issue is a weakness that leaves a company or industry vulnerable to having their data, particularly personal data, breached by an attacker. The six main areas of the NHS IT infrastructure include NHSmail, Summary Care Records, Smartcards, NHS pathways, GP2GP, and Spine [2,8].

Spine connects IT in healthcare with IT in organizations. It's used by 275,000 people each day and if it went down, electronic prescriptions and health records couldn't be accessed or transferred securely which would have an extensive impact because a lot of big data are stored on the system [9].

Another security issue is the NHS using old software. Citrix claims around 90% of the NHS used Windows XP until recently (Interquest Group, 2016). Furthermore, following a cyberattack in 2017, it was revealed that the NHS was given a software patch that would've prevented the attack but failed to implement [10].

Healthcare doesn't consider the "corporate culture" and needs of staff. Staff are allocated smartcards with pins but work in a fast-paced environment where their priority needs to be saving lives and not remembering passwords. Due to this, staff have created workarounds like writing down their passwords. Human error of staff, for example forgetting to logout, is also a factor that could have detrimental effects. If an unauthorized individual gains access to the system and data, it would be a huge security and privacy issue [11].

A final issue is insider threats, employees may exploit their work privilege and gain knowledge which they could use to compromise the security of the company [12].

12.1.3 Challenges in resolving S&P issues

There are many challenges with resolving security and privacy (S&P) issues within healthcare. A major issue, particularly within public healthcare, is lack of funding meaning limited money is spent on improving security. The NHS stated in November this year that another £24 billion is needed by 2022 for patient care to improve and waiting times to decrease [13]. Furthermore, with the NHS employing more than 1.5 million employees and it is challenging to ensure all staff follow the security policy [3,4]. Combined with the mass of data handled and high dependency on "aging infrastructure" such as MRI scanners, this poses new challenges as are difficult to update [14].

12.2 Detailed problem analysis

This section describes specific security and privacy attacks in details that were targeted on UK healthcare in the recent years.

12.2.1 Security attacks

A security attack is an attempt to gain unauthorized access to a website, computer system or network but may not involve getting data. An example is a man-in-the-middle attack [15].

Ransomware attacks infect a computer system or connected devices by encrypting the files until users pay a ransom [16]. One of the biggest ransomware

attacks on healthcare was the 2017 WannaCry NHS attack. This attack impacted over a third of all NHS trusts [17]. It was a security attack due to computer systems in different areas of the NHS being compromised. It could also be considered a privacy attack due to confidential data being accessed.

There's been other attacks on the NHS. In 2017, Barts Health NHS Trust was attacked by a zero-day attack, which exploited an unknown flaw in the system. The attack was classified as a security attack due to malware bypassing software, and getting into the system [18]. In late 2016, a computer virus was directed at Northern Lincolnshire and Goole Hospitals NHS Foundation Trust, getting into the electronic systems resulting in a security attack [19].

12.2.2 Privacy attacks

A privacy attack is an attempt to gain unauthorized access to confidential information and personal data, for example, a data breach [15].

Privacy attacks can be caused by hackers accessing a computer system remotely. As discussed in [6], it has been observed with Harley Medical Group in 2014, where a hacker gained access to 480,000 customer details including, customer names, date of birth, and addresses. Defined as privacy attack as confidential data were released without permission from Harley Medical Group or their customers [9].

In 2011 the hacking group LulzSec hacked the NHS. It was able to penetrate the NHS network which acquires the admin passwords. It was defined as a privacy attack, as confidential admin password was compromised [20].

12.2.3 Impact on enterprise

S&P attacks have the capacity to shut down computers remotely. If these computers are required during life-threatening operations, patients' lives could be at risk. This would also lead to treatments and appointments needing to be rescheduled or delayed, as highlighted in the 2017 NHS attack [17].

Attacks can lead to a lack of trust from clients. This impacted Harley Medical Centre, where lots of competitors offering the same treatments in the private sector, meant customers were likely to move. In privacy attacks, a data breach could impact the financial stability of the enterprise, with the Information Commissioner's Office (ICO) giving out hefty fines for the compromise of data. This would be especially high in healthcare due to the highly confidential data involved [21].

12.3 Proposed solution

This section discusses several tasks to be done in order to develop a strong solution against the attacks discussed in the previous section.

12.3.1 Overall solution description resolving discussed S&P issues

In May 2017, Microsoft provided free software updates to the NHS, as discussed in Section 12.2.1. The NHS had been warned about the risk of cyberattacks over a

year before the devastating WannaCry attack. In the Data Protection Policy by NHS England, current roles and responsibilities for employees are described (NHS, 2016). Outcomes of the WannaCry attack meant “it was not immediately clear who should lead the response and there were problems with communication.” This lack of clear direction resulted in serious consequences [21].

The NHS has set a Data Security and Protection Requirement for healthcare organizations, needing completion by GDPR in April/May 2018. Including, hiring ISOs to establish strategies for the organization and ensure that information assets and technologies are protected correctly [22]. With the addition of a new checklist in place [23]. In response to recent attacks, solutions are needed to protect data as much as possible. Using security solutions with behavior-based detection technologies and engaging in regular penetration and vulnerability testing can help catch ransomware by monitoring how it operates on the system and makes it possible to detect new and unknown ransomware [7,16,24].

The zero-day attack on Barts Health NHS Trust, 2017, solutions could include: keeping up-to-date with patches, fixing vulnerabilities within the software and operating system, and strengthen the resistance to malware attacks [25]. Some solutions for the 2016 computer virus attack on Northern Lincolnshire and Goole Hospitals NHS Foundation Trust would be to review the effectiveness of existing virus/malicious code protection procedures and scheduling regular virus scanning [26–28].

The enterprise NoSQL data platform is being used by healthcare industries to closely monitor sensitive data. Paired with MarkLogic 9, it allows highly confidential information on the data platform to meet cybersecurity requirements. Consumer privacy is safeguarded through advanced encryption methods to protect data, cryptography, and advanced key management [29].

This solution is already in place within the NHS and private healthcare practices as an effective tool in monitoring personal data and employee and customer privacy. This solution combined with two new solutions will work to successfully prevent against S&P attacks. This will increase customer trust and aid staff more efficiently [30].

One of the new solutions is implementation of biometrics within the computer systems and medical equipment. Biometrics is a physiological or behavioral characteristic of a human-being that distinguish one person from another and can be used to verify identity [31].

As discussed in Section 12.1.2, the NHS has an existing system involving a smartcard and pin but by using fingerprint biometrics this will speed up the process. Although implementing biometrics will be difficult and costly and requires maintenance, it's the best solution to fix current issues and is sustainable [4].

The other solution involves updating software and firewalls. Constant updates are required for maximum protection. Although it's currently challenging to update and patch certain medical machinery such as MRI scanners, developers and security teams need to work together in the future to find a fast and secure way to update the machinery. It could be expensive and time consuming to implement and maintain, but it's vital to ensure infrastructure is secure and the cost of mitigating

the risk outweighs the cost of a successful attack. The security of the infrastructure has been targeted in the past and unless a solution is implemented, the issue will continue to rise [21].

These solutions incorporate both old and new security methods which can aid existing technology which shall make future tasks simpler and more secure once implemented. Implementation execution is vital to ensure that all solutions are addressed in the most appropriate manner. To ensure this, the risks prior need to be identified and assessed. The cost of implementation shall depend on the decision to either entirely replace the current authentication platform or add additional biometric authentication to existing security measures, such as aiding swipe card usage, which is the method that suggested most. It is important that the organization investigates the amount of users which shall be on the system, to ensure ease of management. The risk of spoofing is present, therefore before purchasing biometric technology, it is essential that the antispoofing measures are understood [32].

Updating of software and firewalls on systems should be a top priority. This should be undertaken by IT professionals either in-house or outsourced and the cost of installation shall depend on the method used. To reduce disruption, these updates should be undertaken at nonpeak times where systems are less busy or by updating a few machines at a time which means if something does go wrong, the impact is not as severe [33].

Our last solution is firewalls. The cost of implementation depends upon its size and scope. By improving a packet filtering firewall, this allows internal electronic feeds to be filtered along while preventing outside feeds from entering the industries network. This firewalls act as a basis in protecting the security of electronic health records (EHRs) therefore is a critical step. Complex application level gateway firewalls are expensive and time consuming. Therefore, a full internal and external analysis should be done to determine the applicability of the firewall. External network connections are accessed through the gateway in order to prevent external intrusion into the organization's intranet. As a result, it is essential that an assessment is undertaken prior to the decision of the firewalls used, failure to select appropriate options may have disastrous consequences on the confidentiality of information [28].

12.3.2 Resistance against security attacks

Integrating biometrics within the IT infrastructure increases the depth of security. It is difficult to replicate and bypass due to being unique to every individual. This means only those with permission to access computer systems will be able to get in. Unlike with the existing solution of smart cards and pins, these can't be stolen off an employee and memorized by those wanting unauthorized access.

Firewalls should be the first line of defense for every healthcare network, it is critical to aid the protection of any malware penetrating the perimeter of the firewall. It is vital firewalls only allow precleared data to pass through. From an internal perspective, it ensures that employees cannot gain access to harmful public websites which could pose a risk to the system.

12.3.3 Resistance against privacy attacks

As previously discussed in Section 12.2.2, privacy attacks can have detrimental consequences especially in healthcare due to the highly sensitive data that is stored. Collectively, our proposed solutions can effectively resist privacy attacks in comparison to current measures. Implementing biometrics can achieve this as it prevents against unauthorized access to the system therefore having the inability to access sensitive data. Furthermore, if an attacker was somehow able to bypass the biometrics and it will only be able to view basic information, as per the current NHS policy [5].

Firewalls are a protection layer from hackers breaking into the computer system in order to access and steal private files, credit card information, passwords, and identification information [26]. It also prevents internal attacks, reducing human error to some degree. Although the firewalls and software may not fully protect the system as it will minimize the amount of vulnerabilities that can be exploited [21].

The NoSQL data platform and MarkLogic9, discussed in Section 12.3.1, currently exists within the infrastructure and is and will be effective in protecting data. It's incorporated as a solution because this combined with methods previously discussed, will ensure the successful resistance against privacy attacks.

A privacy impact assessment (PIA) has been conducted to identify privacy issues, ensure consumers' expectations are met and data protection obligations have been complied to in the most effective manner possible. It is available to be viewed in Appendixes A1–A6. The privacy impact assessment includes sections on the need for a PIA (Appendix A1), information flow (Appendix A2), privacy risks (Appendix A3), privacy solutions (Appendix A4), PIA outcomes (Appendix A5), and integrating PIA outcomes into project plan (Appendix A6).

The outcome shown in Appendix A6 is the actions to be taken and the completion date to improve current systems and implement new solutions in the future. The completion of all solutions aims to be finished by mid-2021.

12.4 Conclusion and future directions

In conclusion, the attacks experienced in the healthcare industry, highlighted in Section 12.2, have had a vast impact on the reputation of the healthcare industry. It's also important to ensure that the electronic health records (EHRs) are protected due to the volume of patient data contained. After examining previous attacks, the solutions discussed in Section 12.3 indicate ways in which the healthcare industry is able to remain sustainably secure. When discussing the lasting effects for these solutions, biometrics will soon become the norm within industries, taking over from the use of passwords. Using this method means healthcare will be ahead of technological trends. Firewalls and software updates have been used for many years and will continue to protect our systems from intruders. Along with the improved solutions examined, Enterprise NoSQL database platform is the current solution used. This enables the healthcare industry to monitor sensitive data, using a system strictly tailored to their needs.

Appendix A

A.1 Identify the need for PIA

Discussion areas	Discussion points	Answers
Establishing objectives	1. Project aim 2. Benefit of project happening for organization 3. Benefit of project happening for individuals 4. Benefit of project happening for other parties	1. The aim of this project is to identify security and privacy issues within the healthcare industry and create appropriate solutions to combat these issues 2. The organization will benefit because their IT infrastructure will become more sustainably secure, which is necessary in today's cyber landscape as the threat of cyberattacks is increasing rapidly 3. The individual will benefit because their personal data will be more secure due to the solutions suggested which will improve current risk mitigation techniques and decrease the probability of the vulnerability being exploited 4. Other parties, such as the government, will benefit because the healthcare industry is a core part of society, particularly in the UK due to the NHS. A cyber breach or attack has detrimental consequences and affects a lot of people, as proved to be the case by the 2017 NHS hack. So, the mitigation of a cyber breach through the solutions created in this task will benefit the general public as a whole
Screening questions	1. Will the project involve the collection of new information about individuals? 2. Will the project compel individuals to provide information about themselves? 3. Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?	1. N/A 2. N/A 3. N/A 4. N/A 5. Yes, the project involves the implementation of biometrics to improve security 6. May affect individuals because personal data will be more secure. Will impact employees as it will involve implementing biometrics

(Continues)

(Continued)

Discussion areas	Discussion points	Answers
	4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	7. N/A 8. N/A
	5. Does the project involve using new technology that might be perceived as being privacy intrusive?—for example, the use of biometrics or facial recognition	
	6. Will the project result in making decisions or taking action against individuals in ways that can have a significant impact on them?	
	7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations?—for example, health records, criminal records, or other information that people would consider to be private	
	8. Will the project require to contact individuals in ways that it may find intrusive?	
Management support	1. Why is the privacy impact assessment needed?	1. The privacy impact assessment is required to analyze the risks within the healthcare industry, ensure privacy expectations and regulations are met and identify the best solutions that are sustainable. It's also required to ensure aims are met

A.2 Describe the information flow (As shown in Figures A.1–A.3)

Consultation requirements

Deletion of medical records can be undertaken by human resources, although it's not done regularly, after the death of a patient, medical records are kept for a number of years before it got removed from the system. All other personal data would be kept for future records.

An individual's right about the collection, storage, and usage of their data is displayed in the Data Protection Act 1998 and GDPR May 2018.

Table A.1 and A.2 show external and internal consultations, respectively.

Figures A.1–A.3 show information flow of data collection, use of collected data, and its accessibility, respectively.

Collection of data:

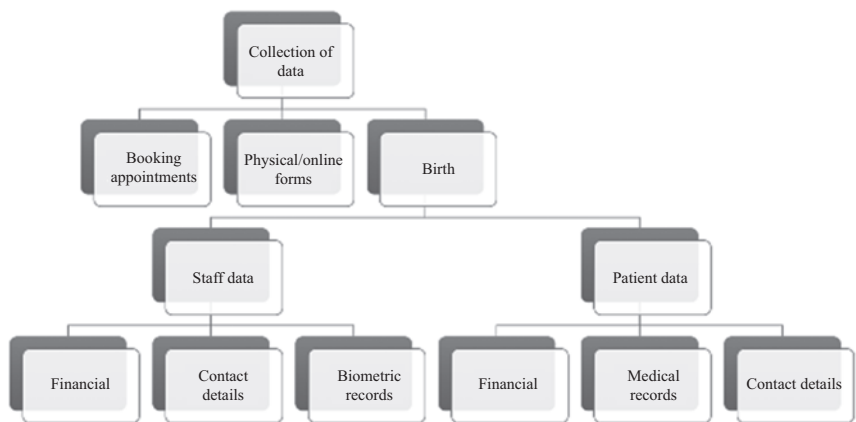


Figure A.1 Categorization of data collection

Use of data:

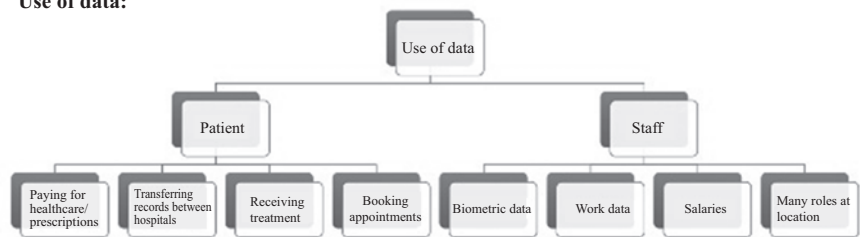


Figure A.2 Efficient use for data within an organization

Who has access to the data

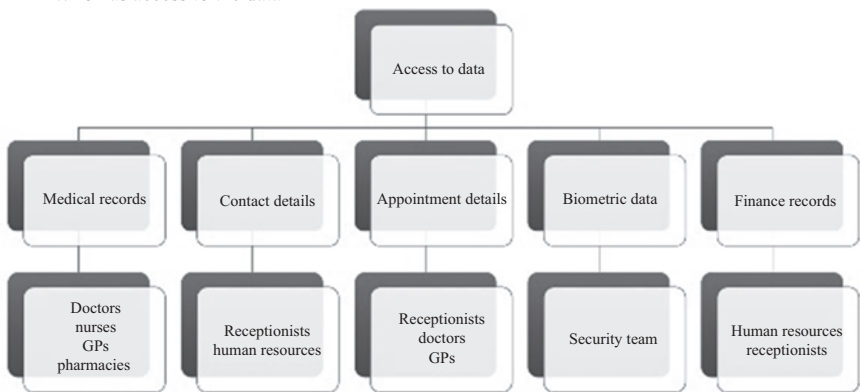


Figure A.3 Accessibility on data

Table A.1 External consultations

Contact	Methods	Achieve
Customers	Emails	To allow customers to be aware of the new security measures which are going to be put in place (biometrics) to increase the security of their data
General public	A public post	Help the general public gain more knowledge. Help the healthcares understanding which aspects need changing, based on the feedback
Management and staff	Meetings	Undertaken to allow staff to understand why their biometric data are needed and how this is beneficial to the organization in order for them to support it. Discuss dates when measurements are to be taken

Table A.2 Internal consultations

Who's contacting	Method	Achieve
Security team	Meetings	To allow the security teams to understand what will be changing in healthcare security. Also, what the new solution involves and how their job requirements are changing for the better, for example using biometrics
Implementation team	Email/meetings	Figure out the final details of the solution and put it in place. Discuss when testing of the new solutions will take place to ensure the work. Then discuss an implementation date along with how often it will be maintained.
Government	Email	Let them be aware of the new changes put in place in the healthcare industry. Discuss why these solutions are going to be implemented
Corporate/senior management	meeting	Discuss solutions to implement. Make sure to understand the costs and benefits of the projects which get being funding

A.3 Identify the privacy and related risks

Privacy issue	Risk to individuals	Compliance risk	Associated organization/ corporate risk
Insider threat — Employees may leak, change, or delete the data,	If the data are changed or deleted there may be no data available or the	Data Protection Act —Personal records being leaked, changed,	Financial loss Money lost due to fines and in private healthcare <i>(Continues)</i>

(Continued)

Privacy issue	Risk to individuals	Compliance risk	Associated organization/ corporate risk
either due to malicious intent or to cover up mistakes	data may be inaccurate Confidential data could be exposed if there is a leak or breach	deleted, or covered up could lead to prosecutions, fines, and enforcement notices for the organization ICO —Leak of data will lead to a fine from the ICO	due to loss of customers/ patients Loss of intellectual property Lost information
External threat — Such as a cyberattack, for example—malware and other cyber threats	Efficiency is disrupted and the performance level is slowed	An ICO — Organization should do all anyone can to protect clients' data and if an attack leads to a data breach, then the organization has obviously been unsuccessful at this	Loss of reputation Loss of government and patient trust if the breach is successful Financial loss The cost of recovering from attack and potential fines from ICO if errors made
Leak of data —May be caused due to internal threat or error or an external threat	Confidential data could be anywhere and seen by anyone. Individuals have no control of what happens to the data	Human Rights Act —Individuals have no control over what happens to information about them Data Protection Act —Currently covered within this act and will be covered by the GDPR when it's released	Loss of intellectual property Data are lost Reputational damage May lose support due to making errors or being unable to mitigate risk effectively
Selling of data — Medical records could be sold illegally	Confidential data could be compromised and be obtained by unauthorized people	Data Protection Act —Personal records have been sold without the owner's permission ICO Fines —Due to data being breached	Financial loss Money lost due to fines caused by a data breach Reputational damage Employee or patient data could be compromised so trust may be lost Loss of intellectual property Medical records stolen

(Continues)

(Continued)

Privacy issue	Risk to individuals	Compliance risk	Associated organization/ corporate risk
Breaking confidentiality confidentiality agreement exists in healthcare to protect patients	Violation of patient confidentiality is a form of betrayal as patients have the right of confidentiality under the law	Nondisclosure agreement broken Nondisclosure and confidentiality agreement broken, organization/individual responsible could be sued Data Protection Act Currently covered within this act and will be covered by the GDPR when it's released	Loss of reputation Patient and government trust lost Possible legal implication Organization could be sued or individuals or private healthcare organizations license to practice medicine could be revoked
Access rights Incorrect allocation of access rights given. Employees being able to access more information than required	Employees may view unnecessary data	Data Protection Act Individuals have the right to know who is allowed to view and use their data	Loss of reputation Customer trust and reputation of healthcare organization lost
Personally identifiable information (PII)	By exploitation if other offenses could be committed, such as fraud	Data Protection Act Exploitation of individuals PII without their consent Human Rights Individuals have the rights to know who sees their PII	Loss of reputation If other offenses are committed and exploitation is publicized

A.4 Identify privacy solutions

Risk	Solution(s)	Result: Is the risk eliminated, reduced, or accepted?	Evaluation: Is the final impact on individuals after implementing each solution justified, complaint and proportionate response to the aims of the project?

(Continues)

(Continued)

Insider threat— Leak the data, change without permission, delete data, and cover up mistakes made	Access rights Track abnormal activity Access vulnerability management solutions— Using a vulnerability scanning to analyze open ports, any infected malware detected on the system Policies against insider threat	The risk cannot be eliminated but can be reduced	The solution has been able to eliminate the risk and therefore has been successful
External threat— Malware (cyber threats)	Firewalls (updating) Penetration and vulnerability testing Antivirus software (updating) Biometric	Eliminating the risk of an external threat, only if these solutions are updated on a regular basis to ensure that it requires up to date system with the evolving skills of hackers Biometrics—Difficult to replicate due to being unique to the individual	These solutions have been successful, only if the updates are on a regular basis and maintained according to the current policies and standards
Leak of data (internal or external threat)	Access rights Correct security software— Identify which devices are being used within the company (BYOD may impact security). These devices must have the latest software installation Training of staff— Ensuring everyone should aware of the importance of protecting corporate data.	The risk should be reduced as employees become more and more educated about the threats to the organizations. With the adequate training for staff in place, it will understand how critical it is to ensure patients' data protected to the highest ability	Risks are reduced and therefore have been successful to the best of their abilities. If these solutions are kept monitored on a regular basis, then the likelihood of data leakages will decrease further and further
Selling of data— Illegal selling of medical records	The only way to prevent this from happening is to prevent individuals from getting	The risk is reduced, but the actual act is out of our control as it cannot monitor the illegal selling of	The risk is reduced as much as possible, but the lack of control that would impact the

(Continues)

(Continued)

	the information in the first place Firewalls—Controls the access that individuals have either internally or externally Biometrics—Stopping unauthorized access NoSQL database platform—Protects the security of the data	medical records and the dealings within. The risk is reduced to the ability as one can but it is accepted in the fact that anyone cannot control the illegal selling	successfulness over the solutions
Breaking confidentiality—Confidentiality agreements in healthcare	Training on security processes Confidentiality policy Access rights—Ensure that only those with the authorized access can get hold of certain information Encrypt as much confidential data as possible—Removable storage devices such as USB sticks and external hard drives	The risk is reduced, because even though training is given to employees, it may not necessarily fully understand or take into consideration the seriousness needed to protect data. This is evident with the confidentiality policy too Access rights also if there are any faults within the system Encryption of confidential data is likely to be mostly a success. However, ensuring the most critical data is the issue	Solutions imposed are able to reduce the risks. These cannot be eliminated as employees may not fully understand the importance of protecting confidential information along with the amount of data which should be encrypted
Access rights—Incorrect allocation	Better management and investigation Biometrics	Risk is reduced as this is not solely possible as there still may be some flaws due to lack in accuracy through checks to ensure all employees are correctly allocated to their specific department Biometrics should also closely be monitor who is accessing areas	The risk is reduced as much as possible, this cannot be eliminated due to human error always being a factor especially when implementing biometrics along with the accuracy of investigating access rights

(Continues)

(Continued)

Personally identifiable information	Educating users Understanding who has access to the data Full encryption of devices— Especially on BYOD Policies for handling data— So employees understand how data needs to be received, handled and stored	The risk here would be eliminated and accepted. As this is a low-cost method, it is easy to implement	Eliminated risk as these solutions are easy to implement

A.5 Sign off and record the PIA outcomes

Risk	Approved solution	Approved by
Insider threat	The solution which will be chosen is access rights. This is a cheaper alternative which requires checking who has access to certain information and if it is actually needed that information in order to do their job. By checking these rights, it will help reduce insider threats as employees will only have the information as needed	N/A
External threat	The approved solution is updating firewalls, in order to have up to date solutions to help protect as much as possible against malware. It also helps monitor ingoing and outgoing traffic, helping it stop malware coming in	N/A
Leak of data	The solution chosen will be correct security software, in order to help it protect from individuals/groups getting in and leaking data. All healthcares already have this solution in place, but some softwares may need updating or changing. The softwares chosen will need to be specific to individual healthcares, due to the different size and budgets which different healthcares have	N/A
Selling of data— Medical records can be sold on the black market	The solution which will be used to try and reduce individuals for getting the data which anyone can then use to sell, is by using biometrics. This prevents individuals getting hold of personal data, which is not been authorize for accessing the computer system or medical records/data Due to this only preventing the internal access to data, firewalls will need to be used. This will try and	N/A

(Continues)

(Continued)

Risk	Approved solution	Approved by
Breaking confidentiality	reduce the risk of individuals getting to the personal data via the firewall, as the firewall monitors the incoming and outgoing traffic Lastly a solution would be to use a NoSQL database platform if healthcare organizations do not already have one. This would allow providing a more secure way to store and retrieve data The solution will be further training on security processes. This will enable its staff to understand the consequences of breaking confidentiality agreements, and the damage it has to the company Another solution will need to be used in order to make sure the confidentiality is not broken, which is encrypting as much confidential data as possible. This is already being done in most healthcares, but needs to be checked	N/A
Access rights	The solution chosen is biometrics, as biometrics can be used to check if the person trying to access the data, actually has access rights to what it is trying to view. This will be done by checking the individual's human characteristics against the system	N/A
Personally identifiable information	Healthcare industries already use policies for handling data. This will continue to be used to make sure the correct data are stored, transferred, deleted, and used correctly	N/A

A.6 Integrate the PIA outcomes back into the project plan

Actions to be taken	Date for completion of actions	Responsibility for action
Updating firewalls —Important to ensure the security of the healthcare industry is maintained. Protecting the network from external and internal threats	Updating firewalls Update the existing system as best as possible—March 5, 2019. For the future, improving the whole system across so many hospitals would take a year and a half to two years to implement—September 9, 2020	Public healthcare Security team— CISO of the NHS and Government Private healthcare Security team and the organization which finances/runs
Biometrics —Ensuring that no unauthorized access to confidential information is gained	Biometrics Implemented in the first hospital within a year—August 19, 2021.	
Updating software —Ensuring that patches are up-to-date to eliminate vulnerabilities within the system and therefore reduce the risk of threats from attackers	Aim to implement across the whole industry as a gradual process as this would be very time consuming	
NoSQL database platform		
Review policies		

(Continues)

(Continued)

Actions to be taken	Date for completion of actions	Responsibility for action
Updating software Update current software as soon as possible. Within a couple of months—February 25, 2019. NoSQL database platform Immediate continuation Review policies In the future. At current, there is no need		

References

- [1] Office for National Statistics, 2017. “UK health accounts: 2015” [online]. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/healthcaresystem/bulletins/ukhealthaccounts/2015> [Accessed May 18, 2019].
- [2] NHS Digital, 2017. “IT infrastructure” [online]. Available from: <https://digital.nhs.uk/article/197/IT-infrastructure> [Accessed May 18, 2019].
- [3] NHS England, 2016. “Information security policy” [online]. Available from: <https://www.england.nhs.uk/wp-content/uploads/2016/12/information-security-policy-v3-1.pdf> [Accessed May 18, 2019].
- [4] NHS England, 2016. “The NHS in England” [online]. Available from: <https://www.nhs.uk/NHSEngland/thenhs/about/Pages/overview.aspx> [Accessed May 18, 2019].
- [5] NHS, 2017. “Registration authorities and smartcards” [online]. Available from: <https://digital.nhs.uk/Registration-Authorities-and-Smartcards> [Accessed May 18, 2019].
- [6] Harley Medical Group, 2017. “Why choose Harley Medical?” [online]. Available from: <https://www.harleymedical.co.uk/why-choose-us> [Accessed May 18, 2019].
- [7] Microsoft, 2017. “Definition of a security vulnerability” [online]. Available from: <https://msdn.microsoft.com/en-us/library/cc751383.aspx> [Accessed May 18, 2019].
- [8] Armentano R., Bhadoria R.S., Chatterjee P., and Deka G.C., editors. *The Internet of Things: Foundation for Smart Cities, EHealth, and Ubiquitous Computing*. CRC Press, USA; 2017.
- [9] Worth, D., 2014. “Hackers hit Harley Medical Group in customer data extortion attempt” [online]. Available from: <https://www.v3.co.uk/v3-uk/news/2340171/hackers-hit-harley-medical-group-in-customer-data-extortion-attempt> [Accessed May 18, 2019].

- [10] Griffin, A., 2017. "NHS Hack: hospitals sent patch that would have prevented chaotic cyber attack" [online]. Available from: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-hack-cyber-attack-patch-hospitals-trust-fix-safety-security-privacy-files-latest-a7736681.html> [Accessed May 18, 2019].
- [11] Sorrentino, F., 2015. "Cyber attacks: 5 ways small businesses can protect themselves" [online]. Available from: <https://www.forbes.com/sites/frank-sorrentino/2015/10/26/cyber-attacks-5-ways-small-businesses-can-protect-themselves/#4d64a10c3193> [Accessed May 18, 2019].
- [12] Center For Internet Security. 2017. "Insider threats: in the healthcare sector" [online]. Available from: <https://www.cisecurity.org/insider-threats-in-the-healthcare-sector/> [Accessed May 18, 2019].
- [13] Campbell, D., 2017. "NHS needs £24bn more by 2022 or waiting lists will grow and care be hit" [online]. Available from: <https://www.theguardian.com/society/2017/nov/08/nhs-needs-24bn-more-by-2022-or-waiting-lists-will-grow-and-care-be-hit> [Accessed May 18, 2019].
- [14] Fearn, N., 2017. "Is healthcare safe from cyber attacks?" [online]. Available from: <http://www.itpro.co.uk/security/28975/is-healthcare-safe-from-cyber-attacks> [Accessed May 18, 2019].
- [15] Techopedia, n.d. "What is an attack?" [online]. Available from: <https://www.techopedia.com/definition/6060/attack> [Accessed May 18, 2019].
- [16] Pope, J. Ransomware: minimizing the risks. *Innovations in Clinical Neuroscience*. 2016;13(11–12):37.
- [17] National Audit Office, 2017. "Investigation: WannaCry cyber attack and the NHS" [online]. p. 6, p. 8. Available from: <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>
- [18] Evenstad, L., 2017. "NHS cyber attack shows need for resilient infrastructure and security education" [online]. Available from: <http://www.computerweekly.com/news/450418779/NHS-cyber-attack-shows-need-for-resilient-infrastructure-and-security-education> [Accessed May 18, 2019].
- [19] Digital Health, 2016. "Virus all but shuts down Northern Lincolnshire and Goole" [online]. Available from: <https://www.digitalhealth.net/2016/10/virus-all-but-shuts-down-northern-lincolnshire-and-goole/> [Accessed May 18, 2019].
- [20] International Business Times, 2011. "LulzSec warn NHS of cyber attack hacking threat" [online]. Available from: <http://www.ibtimes.co.uk/lulzsec-lulz-security-nhs-health-service-cyber-attack-weak-hack-hackers-hacked-sony-nintendo-network-160624> [Accessed May 18, 2019].
- [21] Price, R., 2017. "The NHS has huge security issues and needs to 'get their act together' after the WannaCry attack" [online]. Available from: <http://uk.businessinsider.com/the-nhs-has-huge-security-issues-and-needs-to-get-their-act-together-after-the-wannacry-attack-2017-10> [Accessed May 18, 2019].
- [22] Koppel, R., Smith, S.W., Blythe, J., and Kothari, V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient?. *Studies in Health Technology and Informatic*. 2015;208: 215–220.

- [23] Jay, J., n.d. "NHS England releases new data security requirements for ALL healthcare organisations" [online]. Available from: <https://teiss.co.uk/news/nhs-data-security-requirements/> [Accessed May 18, 2019].
- [24] CSI, 2017. "WannaCry: a response guide to cyber-attacks and ransomware" [online]. Available from: <https://www.csild.co.uk/wannacry-response-guide-cyber-attacks-ransomware/> [Accessed May 18, 2019].
- [25] SOPHOS, n.d. "Zero-day threats guarding against the unknown enemy". [online] Available from: <https://www.sophos.com/en-us/security-news-trends/security-trends/zeroday-threats.aspx> [Accessed May 18, 2019].
- [26] BullGuard, 2017. "Firewall, Internet security, anti virus protection – BullGuard" [online]. Available from: <https://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/firewall-protection.aspx> [Accessed May 18, 2019].
- [27] InfoSec, 2017. "Virus & malicious code, handle virus & malicious code outbreak" [online]. Available from: <https://www.infosec.gov.hk/english/virus/handle.html> [Accessed May 18, 2019].
- [28] Kruse C.S., Smith B., Vanderlinden H., and Nealand A. Security techniques for the electronic health records. *Journal of Medical Systems*. 2017 1;41(8):127.
- [29] Fox, B., 2017. "Is your hospital the next victim of cyber attack?" [online]. Available from: <http://www.marklogic.com/blog/is-your-hospital-the-next-victim-of-cyber-attack/> [Accessed May 18, 2019].
- [30] Interquest Group, 2016. "90% of NHS trusts still operate on Windows XP" [online]. Available from: <https://www.interquestgroup.com/iq-hub/blogs/2016/90-of-nhs-trusts-still-operate-on-windows-xp> [Accessed May 18, 2019].
- [31] Saxena, N., 2017. "Authentication" [online]. Available from: https://mybu.bournemouth.ac.uk/bbcswebdav/pid-1437207-dt-content-rid-7257462_2/courses/076618/ESP-Authentication%20-%20202.pdf [Accessed May 18, 2019].
- [32] Rubens, P. How it works Biometric authentication. *eSecurity Planet*. 2012. [online]. Available from: <https://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html> [Accessed March 2019].
- [33] Bodkin, H., Henderson, B., Donnelly, L., Mendick, R., Farmer, B., and Graham, C. Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms. *The Telegraph*. 2017;13:2017.

This page intentionally left blank

Part III

The role of blockchain to maintain security and privacy in healthcare

This page intentionally left blank

Chapter 13

Blockchain-based health information privacy protection

Quanxin Zhao¹

General healthcare-related information and data of patients can be recorded from treatment, healthcare operation, and payment. Privacy is the primary determinant to adopt and utilize patients' health information successfully, which requires to be secured and protected by both individuals and organizations. Although current essential guidelines in the domain of health information privacy include information protection law, security and healthcare record standards, professional ethical consensus, etc., there still exists a great threat for protecting patients' healthcare information from loss, theft, and hacking, which leaves securing privacy an important and tough issue. The up to date technology has great potential to solve above tough issue within the existing healthcare information privacy frameworks and approaches, which can be realized and implemented through the control, manage, and protect of patients' healthcare information data in order to answer the following questions, such as who can access the information, how to see and protect the data record, and how to make sure the data correct. The promising blockchain has an explosive increase in the use cases of healthcare, which technology is a decentralized digital shared ledger with each block containing data records related to patients' health information. The data in the entire blockchain can be easily validated and verified by massive ordinary computers in many locations of the world, making the patients' health information and data almost impossible to make illegal changes without being permitted or detected. The blockchain has many unique technical characteristics compared to existing other technologies and will make a deep impact on keeping health information privacy, which raises major challenges that demand holistic approaches to deploy and use such novel technology. The contribution of this chapter lies in, by exploring blockchain technology facing health information privacy and finding a detailed framework and practical examples, the optimal design of blockchain is proposed to address the privacy of patients' health information and data from the following aspects, such as technological frameworks, theoretical model, technical approaches, and performance evaluation metrics.

¹Sichuan Netop Telecom Co., Ltd., Mianyang, China

13.1 Basic concepts

13.1.1 Health information

Data of health, medical, and clinical are health information, which is usually produced by people such as patients, clinicians, doctors, and physicians for the aim of comparative studies, healthcare operation, life science research, treatment, payment, policy assessments, etc.

13.1.2 Health-related data privacy

Information privacy has a close relation with collecting and disseminating data legal and political issues, coming up from the process of data collection, data stored, data usage, and data destroyed or deleted.

13.1.3 Blockchain in healthcare

The blockchain works as a decentralized digital shared ledger and produces multiple computer-stored copies. Any blockchain in any location of the world can verify the validation of the entire blockchain. There are types of blockchains covering massive healthcare use cases, which stakeholders including administrators, customers, institutions, patients, providers, etc.

13.2 The process of health information and data

13.2.1 Participants in healthcare and e-healthcare

The main components in the medical include patients, providers, payers, and vendors, which are described below. First, patients are the medical care received individuals. Second, providers are the institutions buying products from vendors, charging payers, and giving medical care to patients. Third, payers are the institutions paying providers for their healthcare services. The providers include the government, individuals, insurance carriers, and private employers. Last, vendors sell pharmaceutical products, medical care devices, services, and solutions to providers.

13.2.2 Authentication and access for health data

It is important to prevent unauthorized access to medical care data. To satisfy such security requirements, it can either assign patients' own rights at their discretion to give medical care data access to others or arrange authorization data access control rules.

Authorization is important for making sure the information of patients' health in terms of both the security and the privacy. The dynamical environment of information access is constantly changing for making the authorization issue more complicated, giving applications the opportunity to import context awareness for providing enhancement and valuable usage.

The authorization model permits for accessing control exemplification on the basis of attribute. These permissions of information resources are associated with some rules for the measurable attributes of information resources, systems, users, etc.

Large networked healthcare systems manage and control patients' data for diverse purposes. In the healthcare industry, there always exist effective data access management by implementing a variety of policies of access control. Further, there also exists noticeable improvement in key technical solutions to data access management and health organizations, giving broader access privileges to facilitate timely and effective healthcare. Some specified technology has implemented a module of policy refinement for periodically examining the access logs and identifying policy rules with sophisticated data-mining.

13.2.3 Storage and maintenance in health data

The material of patients' medical care includes charts, images, physicians' notes, etc. According to a report, the volume of healthcare data will reach 2,314EB by the year 2020, challenging for data storage issues, which storage of healthcare data can be the cloud, flash, and the emerging blockchain technology.

Usually, healthcare organizations will have their own storage needs, such as smaller organizations prefer traditional disk-based storage, while larger hospitals or health systems which handling a larger amount of data prefer the cloud and the emerging blockchain technology.

13.2.4 Protection and recover for health data

The increasing volume of health data can be a major concern for disaster recovery. Up till now, there is lacking executing suitable protection. To evaluate the disaster recovery, it can take six best practices into consideration, such as the plan for redundancy, trust but verify, plan for accessibility, be compliant, be prepared, and think scalable. These best practices are described below.

First, three copies of data on two different media should be sure so that there will be at least one copy maintained off-site. Second, it verifies the backup data each night and does testing the recovery files from the backup periodically. Further, it could be sure that the backup data are working properly at any time. Third, before encountering business interruption, it always allows people to work remotely and gives immediate critical data access through backup systems. Forth, as business becoming highly regulated, providing the same level of compliance as core systems is very important for both IT vendors and backup systems. Fifth, it is important to design and test the disaster recovery plan to confirm that putting the predefined plan into action is ready at any time. Sixth, as the growing of generated data, the capacity of backup is considered to grow with the volume of generated data.

13.2.5 Case studies in health information privacy

Taking UC Davis Health System (UCDHS) as an example, which system utilizes electronic health record, which is termed as electronic health record (EHR), for

providing and/or recording many kinds care of medical and care of clinical from some organizations, which includes ambulatory, encounters, home care, inpatient, and telehealth. For the EHR, which can make contribution to the providers of both affiliated and nonaffiliated community-based healthcare in the way of direct healthcare data access and exchange, patients with their family members who are authorized for the aim of reading/writing to clinical data directly in the personal health record (PHR) which is EHR tethered.

In order to obtain the equilibrium between the safeguard of protected health information, which is termed PHI, and the avoidance of excessively limited access management and control for not interfering with the care of patients, it creates the multifaceted Privacy and Security Program, which holistic scheme is taken by UCDHS. In addition, a few innovative processes with the corresponding tools of software is set up by UCDHS for managing access to clinical content.

Significant investments have been made by the organization in emerging privacy and security technology. This technology has the characteristics as shown in Table 13.1.

1. Knowledge of background

The privacy of patient data has been regarded as the key priority of organizational, which is done by UCDHS, UC Davis with some characteristics is shown in Table 13.2.

The program of clinical privacy by UCDHS consists of distinctive regions relating to the access that EHR managed, surveillance tools with audit trails. Healthcare providers from conferences, Epic user group meetings, and forums are very interested in this comprehensive scheme because it can provide privacy as well as security.

Table 13.1 Characteristics of the technology

Number	Content
1	Secure computer backup media, relevant emails, and thumb drives
2	Unusual for healthcare providers
3	With an unusual focus on encrypting client computers

Table 13.2 Characteristics of UC Davis

Number	Content
1	Locally created policies
2	Software and commercially available technologies
3	Workflow

2. Local problems with planned improvement

The complex huge medical center of academic, UCDHS gives much attention to privacy and security and compliances with explosive increasing regulatory mandates. The work it has done includes protecting sensitive information as well as patients who are facing high risk. The aforementioned information can be especially challenging, which are genetic predictive testing, HIV, and self-pay visits. What's more, it concentrates on both engaging patients with their families to decide and manage care, and improving caregivers' communication, generated a series of new security concerns, as well as opened EHR new portals of access.

It is a tough challenge to manage the privacy and security of over two million patients in the EHR, over eight thousand clinical EHR users, over two thousand community-based users such as reviewers, researchers, referring physicians, and telemedicine users. Further, it is also hard to process and track nearly over 100 thousand managed PHI disclosures for each year. The prior process cannot make sure that it can satisfy the level of security requirements for the organization, which process is list in Table 13.3.

It requires the organization's changing approach to its security and privacy in order to give millions of patients' privacy records' protection. Its aim is for making sure that the privacy of PHI is protected and potential for material breaches is eliminated by UCDHS.

3. Design and implementation

It should form a committee of the Compliance Officer, Human Resources, HIM and IT, Legal Counsel, Privacy and Security Officer, and Risk Management, before designing the program. For providing the protections in terms of security and privacy under no impeded patients' care, this is the focus of the starting philosophy. Moreover, obeying by both state/federal statutes and organizational policies, users of EHR will be held personally accountable for, which is made clear by UCDHS. Below are summarized remaining programs with key aspects in the area of privacy and security.

13.2.5.1 EHR centralized systems with security control

UCDHS is applied for building up systems with the characteristics of automated provisioning, centrally managed but unique, which kind of systems are coupling role-based access matrix of Epic EHR's security, reducing supported staff for exception manual intervention. Currently, on the basis of the user's job credentials,

Table 13.3 The prior process

Number	Content
1	Fragmented in clinical silos
2	Labor-intensive
3	Plagued with unmanageable numbers of templates for the security of EHR

department, and title/functions, the provisioning system can complete the request automatically, which can be done once,

- (a) authorizing the IT system access request by a manager and
- (b) providing proof of identification, HIPAA training as well as user-signed statement of confidentiality.

13.2.5.2 Surveillance program of EHR

UCDHS designed a system of surveillance, that is centralized as well as a one-of-a-kind. In this system, it performs both complaint investigations and risk-based privacy surveillance routinely. For the example of privacy surveillance concentrations with the periodic detective, it is important for accessing to co-workers, EHR users' relatives, hospitalized employees, HIV and psychotherapy patients, high-risk patients, or users of technology to access the patient's data under the conditions of nonproduction. It also develops a method, which innovative method concentrates on timely monitoring the access of the user to the content of EHR. Such the process of surveillance will not only support timely monitoring high-risk patients' EHR activity but track all EHR transactions in terms of the dates, locations, times, and users.

13.2.5.3 EHR privacy of sensitive information

Providing extra safeguards for patients as well as their recorded data, there are a few ground-breaking technologies:

(a) Alerts of security system

Customized "Break-the-Glass" and "Patient Highlights" are designed to dissuade privacy violations. Moreover, the aim of design also focuses on high-risk patients EHR, sensitive information patients, visiting restrictions patients, and victims of identity theft. When an unauthorized user requesting reading to one of these patients' record, "Break-the-Glass" occurs. It requires the user both writing the reason to read the record and re-entering the password. The user cannot continue their workflow until after being authenticated. For potential investigation further, request log will be created and reviewed.

(b) Privacy and security protections for genetic testing

The innovative process of Enhanced Medical Information Security (EMIS) is introduced by UCDHS for providing secondary protection against inappropriate disclosures, otherwise, which will lead to potential discrimination. For requesting Huntington's disease predictive testing, patients will be assigned the name of pseudonym patient. In addition, to obtain additional privacy protection, Break-the-Glass functionality will be used.

(c) Security access restrictions for psychotherapy notes

By marking sensitive notes, system functionality permits clinicians sequestering psychotherapy notes, which technical is further applied for safeguarding the notes of ultrasensitive. In summary, UCDHS utilizes this technology for restricting access to notes merely for psychotherapy security approved individuals.

13.2.5.4 Risk assessment for EHR HIPAA

In the independent Internal Audit Department, UCDHS consists of two IT auditors. Such department both analyzes technology infrastructure of the health system's and performs audits with highly detailed in order to find out potential risks and gaps of security. IT leadership not only cooperate with both the Compliance Department and Internal Audit but guarantee to accomplish an EHR risk assessment by a third-party audit firm.

13.2.5.5 Process on technology evaluation

To evaluate technologies prior to implementation and purchase, the process is implemented by UCDHS, which aim is to make sure that the technology can satisfy the requirements of security and infrastructure support. The application area of this process can be new clinical devices, new infrastructure, and new service providers. The prospective technology vendor can complete evaluations, such as a security questionnaire. There are over 60 questions in the security questionnaire, which content focuses on key risk issues, including the operator of application hosting, data with its flow, third-party background checking, and many others such as physical security, access, encryption, and authentication. It requires UCDHS Purchasing to get results from the process of evaluation, before buying all technology in scope.

13.3 Laws, policies, and standards

13.3.1 Privacy legal protection with laws

Privacy and security of the e-Healthcare data consist of some high-level elements, including the law, professional ethical consensus, and policy guidelines.

Governed by the law, general health information's privacy and confidentiality are often to manage the providers of collocated and integrated care, which can tell how to share health information.

13.3.2 Practical examples of privacy policies

Privacy laws and international privacy standards need companies to gather the data that they have stated the purpose before. Furthermore, these regimes prescribe that companies cannot utilize the collected data with the purposes other than the previous purposes which they have previously gathered. To help companies design high-quality public privacy requirements, a case study is conducted to identify how to express their intended purpose. This taxonomy and the patterns can much help policy analysts for much better complying with the principles of both gather and utilization limitation.

A case study will be conducted to understand how to publish healthcare data purpose by companies within their own policies of data privacy. In such case study, it will seek to identify and categorize purposes of healthcare data, study the variations in purposes of data, and analyze the scenarios, which data purpose can be guessed from both information types and actions.

There exists an analysis of privacy policies with the corresponding purpose annotations of produced data, which can further be categorized into six categories and describe below.

- (a) **Service purpose**
A company can often take actions such as advertisements, preference-based content, website services improvement, etc., with the purpose of providing services to users.
- (b) **Legal purpose**
Companies take actions such as for purposes of regulatory and orders of the court, with any legal purpose for both court order and regulatory requirements.
- (c) **Communication purpose**
Companies can take actions to communicate products, provide services, propose issues, give notifications, update with users, with the purpose to respond user queries, resolve issues from user contact, and update about new products.
- (d) **Protection purpose**
Companies take actions such as the purpose of both fraud detection and user-data protection, with the purpose to match the detected healthcare data to a machine and to make sure that an authorized machine has transferred the healthcare data.
- (e) **Merger purpose**
Companies can often act on a type of information with the purpose for the case of mergers, transfer company assets, and control.
- (f) **Vague purpose**
Companies can often act on a type of information with the vague purpose unclear for the consequence and reason.

13.3.3 Standards in the area of privacy and security

On the international level, security and privacy can be divided into some core elements, which have been agreed. The abovementioned elements are defined in the ISO standard.

ISO/TC 215 standards includes the ISO CODE such as ISO 17090-1:2008, ISO 17090-2:2008, ISO 17090-3:2008, ISO 22857:2004, ISO 27799:2008, ISO/TS 22600-1:2006, ISO/TS 22600-2:2006, ISO/TS 25238:2007, ISO/TS 21089:2004, and ISO/TS 27809:2007.

TC 215 ISO/IEEE standards includes ISO/IEEE code such as 11073-10101:2004, 11073-10201:2004, 11073-20101:2004, 11073-30201:2004, 11073-30301:2004, ISO 11073-90101:2008, and ISO/HL7 21731:2006.

TC 215 ISO standards includes ISO code such as 17090-1:2008, 17090-2:2008, 17090-3:2008, 17115:2007, 13606-1:2008, 17432:2004, 18104:2003, 18232:2006, 18812:2003, 20301:2006, 20302:2006, 21549-1:2004, 21549-2:2004, 21549-3:2004, 21549-4:2004, 21549-5:2004, 21549-6:2004, 21549-7:2004, 22857:2004, and 27799:2008.

TC 215 ISO/TC standards includes ISO/TC code such as 11073-92001:2007, 12052:2006, 16058:2004, 17117:2002, 17120:2004, 18308:2004, 21091:2005, 21667:2004, 22600-1:2006, 22600-2:2006, and 25238:2007.

TC 215 ISO/TR standards includes ISO/TC code such as 16056-1:2004, 16056-2:2004, 17119:2005, 18307:2001, 20514:2005, 21089:2004, 21730:2007, 22221:2006, 22790:2007, and 22809:2007.

13.4 Healthcare IT systems

13.4.1 *Current privacy in healthcare IT systems*

Security and privacy of the system have key elements including locally defined access rights, rights of security and privacy based on locally agreed policies, and outsider access via the human agent.

There are three kinds of HIS, which is illustrated below.

- (a) Organization-centered e-HIS, which is the most popular current system and can span an organization and easy to offer the mechanisms of external access.
- (b) Process-centered HIS, which is to facilitate patient care process among many organizations, as there is an increasing trend to change from organization-centered one to process-centered one. Further, an inter-system communication of e-Healthcare information helps patients transferring from one healthcare organization to another.
- (c) Person or patient-centered HIS, which is expected to change from the process-centered one into the person or patient-centered one. Moreover, the patient can directly involve in the e-Healthcare information of creation, control, ownership, and maintenance.

13.4.2 *Technical solutions to secure privacy*

The importance of technical features is consent mechanisms, and mandated access control policies. To satisfy security and privacy requirements, patients in health information systems will be given with consent, scalability, and interoperability. It is imperative to define access control policies and strategies to ensure security, through which, it can provide patient data proper confidentiality and access rights to.

13.4.3 *IT security challenges and case studies*

Security challenges in each sensitive-based application can be always analyzed on the basis of certain requirements of security, as shown in Figure 13.1.

For the identity proof, it is a necessary system component to process the information of confidential by introducing technique of authentication. All of which can communicate with the system with a few mobile devices.

To decide if a user/system can start an activity, reading/writing to a file, for example, authorization becomes the act of determining. According to his/her credentials, a view of the system can be accessed by him/her if he/she is system

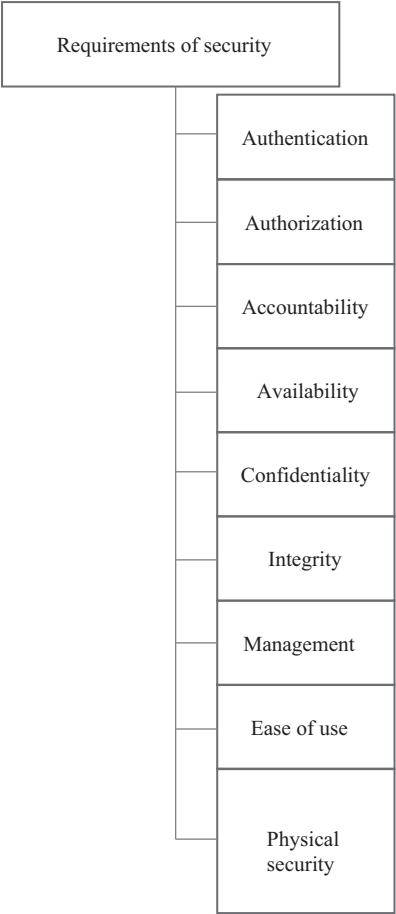


Figure 13.1 Requirements of security

authenticated. Regarding to the job function system, it assigns the user appropriate permissions for reading/writing to specific information.

To answer for actions and track down appropriate authority, individual’s misuse case is easy to be found by accountability. When performing a job without mistake, all members should answer their actions and need to be legally covered.

It is possible for availability loss when the information or systems becoming inaccessible.

Confidentiality enables authorized people to access available information. According to the confidentiality of medical and laws of data protection, it enables the information confidentiality of healthcare systems protecting the patients’ data. The intended recipient can be delivered the exchange of system information. To be

legally covered in a lawsuit, it is important to store and process patients' personal data by writing patients consent.

When exchanging in the network with insecure characteristic, it is important to alter information, since utilizing inaccurate information can be disastrous. Outside of the expected way, it can make sure that integrity controls cannot alter information. So, transporting the information process cannot be intercepted or modified from one to the other.

When the system is working, it is needed for handling and responding to any occurred problem by comprehensive administration. When the system encounters a problem, the presence of a person can give great help. Procedures should be maintained by the administrator to find problems of system operation with corresponding respond action.

The healthcare team has a close concern with the physical risks which relate to the access to the wireless devices. Using wireless devices can pose the system great threat because the wireless device can carry off sensitive information easily.

13.5 Blockchain solutions for health information privacy

13.5.1 Blockchain impact on health information privacy

A blockchain works as a record book, in which lines will include transactions, which represent all the transactions added in the blockchain. There are multiple copies of blockchain saved on electronic devices in the world; moreover, each can both verify and validate the whole blockchain.

There exist many types of blockchains, moreover, there are a few use-cases on the technology of blockchain in the area of healthcare. To consider blockchain affecting healthcare, it will be classified into two primary kinds, namely, trustless and permissionless. The blockchain can afford the innominate cryptocurrencies transaction and electronic asset.

The new kinds involve self-sovereign identity and the smart contract. Further, apart from existing boundaries, it will be extended to pre-existing trust in terms of the health system for both patient and provider.

The above components have quicker interoperability among healthcare systems and also have scale efficiently for processing a large volume of data and users. Blockchain can permit to access shared source of data of healthcare for obtaining comprehensive, precisely and timely patient health data. Combined with lakes of data, data structures of blockchain can enable a large sources of health data, such as information coming from patient documents, images, mobile device applications, sensors, etc. The other blockchain advantage in terms of the distributed architecture can be both disaster recovery and fault tolerance. Since healthcare data are distributed across a few servers at diverse locations of the world, there will not be any single-point failure; further, it's not easy to make a bad impact on the whole world locations simultaneously.

13.5.2 *Technological frameworks*

For the technology of peer-to-peer distributed ledger, blockchain consists of several primary components, including decentralized networks, digital transactions, and the shared ledger. Blockchain operates on the decentralized peer-to-peer architecture. Each network node stores a unique blockchain, contributing to digital transactions in terms of certifying and validating. Such distributed network's nodes use shared ledgers to record electronic transactions. The network node runs some solutions to verify and evaluate certain digital transactions. Such new transactions will not be added to the shared ledger until the validation of transaction is confirmed by most network nodes. After adding a transaction, it will be reflected for all network nodes in all copies of the blockchain, therefore, it will be constant and cannot be removed or changed anymore. Notice that any type of data will be saved in blockchain. Besides, information can be signed and even encrypted in order to make sure precisely, determined data authenticity and information accuracy. Transactions are structured into blocks while each one holds an encrypted hash to the prior one.

13.5.3 *Performance evaluation metrics for security and privacy*

All environment parameters of software testing, such as workload, could be recorded. Below, there are a few additional considerations under the consideration of environment assess where performance evaluation can be started.

- (a) Consensus protocol can be applied in the process of testing, for example, Practical Byzantine Fault Tolerant, which is termed as PBFT.
- (b) Nodes' geographic distribution describes network setup, such as either collocated or dispersed geographically for all the nodes.
- (c) All peers' hardware condition indicates some parameters including a number of cores, running rate of the processor, the volume of memory, etc.
- (d) The network is data related to network complexity among network peers. This can be revealed potential highlighted bottlenecks. It is important to know the type and number of firewalls to be traversed. It shall call out any kind of complex network components.
- (e) For the nodes that are related to the transaction, it will broadcast the transaction on the platform of blockchain to all network nodes, on the contrary, other nodes limit the exchange to the nodes of network.
- (f) Tools for testing purpose with its framework demonstrate which tool to be utilized, besides, what kind of framework for testing purpose can be designed to produce results of the load. Further, it can describe how to drive the test load, and analyze the relationship between the load driver position and the node in the platform.
- (g) Data store type can take an effect on the store, which affecting property when including both writes and reads. Moreover, the platform will provide the underlying ledger data store with a few pluggable choices, such as Postgres, H2, CouchDB, and primary vendors' databases.

- (h) The Workload is the software code, which is designed to both validate and create the transaction. Such characteristics are going to be marked as results of testing, as comparing performance tests across platforms is becoming easier.

Several blockchains common metrics, along with a mathematical formula are defined below.

Read Latency is defined as the time when the response received minus the submit time. Such metric is defined as the moment when submitting the reading request minus the reply receiving moment.

Read Throughput is defined as the total read operations over the total time in seconds. Such metric represents the number of completed reading operation within certain delay of time with the unit, reads per second which are termed as RPS.

Transaction Latency is defined as the confirmation time at network threshold minus the submit time. Such metric is the time waiting for the transaction becoming available for the entire network from the view of network-wide. The measurement consists of the data propagation time and consensus mechanism settling time.

Transaction Throughput is defined as the total committed transactions over total time in seconds at the number of committed nodes. Such metric represents the percentage of success for the transactions that committed and validated within a certain time, which is operated by the blockchain SUT. This rate within a network-size wide can be expressed as transactions per second (TPS). Remember that the total committed transactions are calculated from total transactions minus the total number of invalid transactions.

Below blockchain performance metrics may offer interesting insights.

Blockchain work is defined as the function of both the transaction throughput and the network size. Such metric, meaningful performance characterization, is a function with parameters including the throughput of transaction and validating consensus nodes number. This metric is proposed for the blockchain network to represent the amount of accomplished work. Taking a blockchain with one node into consideration, this can improve throughput but cannot afford availability or integrity guarantee.

Further reading

- [1] Rezaeibagha F., Win K. T., and Susilo W. "A systematic literature review on security and privacy of electronic health record systems: technical perspectives." *Health Information Management Journal*, 2015; 44(3): 23–38
- [2] Braunstein M. L. *Health Informatics on FHIR: How HL7's New API is Transforming Healthcare*. Switzerland: Springer International Publishing; 2018
- [3] Shoniregun C. A., Dube K., and Mtenzi F. *Electronic Healthcare Information security*. New York: Springer Science & Business Media; 2010
- [4] Robichau B. P. *Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records*. New York: Apress; 2014

- [5] Gibbons M. C. *eHealth Solutions for Healthcare Disparities*. Switzerland: Springer Science & Business Media; 2007
- [6] Wickramasinghe N., Bali R., Suomi R., and Kirn S. *Critical Issues for the Development of Sustainable e-Health Solutions*. Switzerland: Springer Science & Business Media; 2011
- [7] Koutsouris D. D., and Lazakidou A. A. *Concepts and Trends in Healthcare Information Systems*. Switzerland: Springer, 2014
- [8] Bichindaritz I., Vaidya S., and Jain A. *Computational Intelligence in Healthcare 4: Advanced Methodologies*. Berlin: Springer; 2010
- [9] Amirian P., Lang T., and Van Loggerenberg F. *Big Data in Healthcare: Extracting Knowledge from Point-of-Care Machines*. Switzerland: Springer; 2017
- [10] Vitabile S., Marks M., Stojanovic D., *et al.* "High-performance modelling and simulation for big data applications." *Medical Data Processing and Analysis for Remote Health and Activities Monitoring*. Switzerland: Springer, Cham; 2019: 186–220
- [11] Casado-Vara R., and Corchado J. "Distributed e-health wide-world accounting ledger via blockchain." *Journal of Intelligent & Fuzzy Systems*, 2019; 36(3): 2381–2386
- [12] Monteil C. *Blockchain and Health*. Digital Medicine. Springer, Cham; 2019. pp. 41–47
- [13] Roehrs A., da Costa C. A., da Rosa Righi R., da Silva V. F., Goldim J. R., and Schmidt D. C. "Analyzing the performance of a blockchain-based personal health record implementation." *Journal of Biomedical Informatics*, 2019; pp. 103–140
- [14] Chen L., Lee W. K., Chang C. C., Choo K. K. R., and Zhang N. "Blockchain based searchable encryption for electronic health record sharing." *Future Generation Computer Systems*, 2019; 95: 420–429
- [15] Zaghloul E., Li T., and Ren J. "Security and privacy of electronic health records: decentralized and hierarchical data sharing using smart contracts." *International Conference on Computing, Networking and Communications (ICNC)*. Honolulu: IEEE; 2019. pp. 375–379
- [16] Tang F., Ma S., Xiang Y., and Lin C. "An efficient authentication scheme for blockchain-based electronic health records." *IEEE Access*, Australia, 2019; 7: 41678–41689
- [17] Jyothi E. V. N., and Rajani B. "Effective handling personal electronic health records using metadata over cloud computing." *First International Conference on Artificial Intelligence and Cognitive Computing*. Springer, Singapore; 2019. pp. 415–426
- [18] Winter J. S., and Davidson E. "Big data governance of personal health information and challenges to contextual integrity." *The Information Society*, 2019; 35(1): 36–51
- [19] da Silveira F., Neto I. R., Machado F. M., da Silva M. P., and Amaral F. G. *Analysis of Industry 4.0 Technologies Applied to the Health Sector: Systematic Literature Review*. Occupational and Environmental Safety and Health. Springer, Cham, 2019; pp. 701–709

- [20] Bandopadhyay S., Murthy G. V. S., Prabhakaran D., Taylor P., and Banerjee A. "India and the United Kingdom—what big data health research can do for a country." *Learning Health Systems*, 2019; 3(2): e10074
- [21] Nalin M., Baroni I., Faiella G., *et al.* "The European cross-border health data exchange roadmap: case study in the Italian setting." *Journal of biomedical informatics*, 2019; 94: pp. 1–11
- [22] Peters R., and Meesters B. *Heathlands of Digital Health Compliance*. Pharmaceutical Care in Digital Revolution. Switzerland: Academic Press, 2019; pp. 195–210
- [23] Talal M., Zaidan A. A., Zaidan B. B., *et al.* "Smart Home-based IoT for Real-time and secure remote health monitoring of triage and priority system using body sensors: multi-driven systematic Review." *Journal of medical systems*, 2019; 43(3): pp. 1–34
- [24] Wang X., Zhang A., Xie X., and Ye X. "Secure-aware and privacy-preserving electronic health record searching in cloud environment." *International Journal of Communication Systems*, 2019; 32(18): e3925
- [25] de Carvalho Junior M. A., and Bandiera-Paiva P. "Unwanted RBAC functions over health information system (HIS)." *International Conference on Information Technology & Systems*. Springer; Cham, 2019. pp. 712–719
- [26] Nayak B., Bhattacharyya S. S., and Krishnamoorthy B. "Democratizing health insurance services; accelerating social inclusion through technology policy of health insurance firms." *Business Strategy and Development*. 2019; pp. 1–11
- [27] Rouse W. B., Johns M. M. E., and Pepe K. M. "Service supply chains for population health: overcoming fragmentation of service delivery ecosystems." *Learning Health Systems*, 2018; pp. 1–9
- [28] Kumari A., Tanwar S., Tyagi S., and Kumar N. "Fog computing for Healthcare 4.0 Environment: opportunities and challenges." *Computers and Electrical Engineering*, 2018; 72: pp. 1–13
- [29] Vora J., Nayyar A., Tanwar, *et al.* "BHEEM: A Blockchain-based Framework for Securing Electronic Health Records." *IEEE Global Communications Conference (GLOBECOM)*. IEEE; 2018. pp. 1–6
- [30] Vora J., DevMurari P., Tanwar S., Tyagi S., Kumar N., and Obaidat M. S. "Blind signatures based secured e-healthcare system." *International Conference on Computer, Information and Telecommunication Systems (CITS)*, IEEE; 2018. pp. 177–181
- [31] Hathaliya J. J., Tanwar S., Tyagi S., and Kumar N. "Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach." *Computers & Electrical Engineering*, 2019; 76: pp. 398–410
- [32] Vora J., Tanwar S., Tyagi S., Kumar N., and Rodrigues J. P. C. "FAAL: Fog computing-based patient monitoring system for ambient assisted living." *IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE; 2017. pp. 1–6
- [33] Vora J., Italiya P., Tanwar, *et al.* "Ensuring Privacy and Security in E-Health Records." *International Conference on Computer, Information and Telecommunication Systems (CITS)*, IEEE; 2018. pp. 192–196

- [34] Tanwar S., Thakkar K., Thakor R., and Singh P. K. “M-Tesla-based security assessment in wireless sensor network.” *Procedia Computer Science*. 2018; 132: 1154–1162
- [35] Tanwar S., Obaidat M. S., Tyagi S., and Kumar N. “*Chapter 10: Online signature-based biometrics recognition,*” *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG 2019. pp. 255–285
- [36] Tanwar S., Tyagi S., Kumar N., and Obaidat M. S., “Chapter 21: Ethical, legal, and social implications of biometrics technologies.” *Biometric-Based Physical and Cybersecurity Systems*, Springer Nature, Switzerland AG 2019. pp. 535–568

Chapter 14

The importance of healthcare information privacy through blockchain

*Dhananjay Kumar¹, Sharmila Arun Kumar¹,
Pramod Kumar¹,
and Mohd Helmy Abd Wahab²*

Healthcare information contains highly delicate and hypersensitive private data, and it needs to be shared among the people such as health specialists, pharmacists, patient's family members, insurance agencies, hospitals, and governments very often. The common mass is not aware of true assessment and importance of the medical data and do not have access to their own medical records at times while healthcare providers and regulatory authorities can make profitable insights from those data. Beside these due to intensive generation of health-related data and the need of its frequent circulation, the storage, and computing of these highly voluminous data are being shifted on latest computing platforms like cloud computing and Internet of things (IoT). These advanced technological developments have eroded the privacy and integrity of such highly sensitive personal data. Also, Artificial Intelligence (AI) technologies like transfer learning and deep learning are capable of modeling normal imagery or recorded data of a person into insight full therapeutic data which also put a threat of private data being recorded without the consent of the concerned person. This extended accessibility to health data presents remarkable opportunities for deploying security measures and predictive analysis mechanisms in healthcare sector. Healthcare organizations not only have their patient's medical investigations details but also record their account information for taking care of treatment and insurance related financial transactions. That is why the mitigation of risk of security breach of healthcare information becomes one of the most crucial aspects of healthcare data management. The extensive research works are being carried on to ensure the security of advanced healthcare systems such as electronic medical report (EMR), electronic health records (EHR), health information system (HIS), and personal health records (PHR).

¹Department of Computer Science Engineering, Krishna Engineering College, Ghaziabad, India

²Department of Computer Engineering, Universiti Tun Hussein Onn, Batu Pahat, Malaysia

Recent researches show a variety of algorithms proposed based on encryption techniques by various researchers but traditional cryptographic techniques and security methods fail to take care of access control and confidentiality of the sensitive health data on cloud, fog, or other modern computing and storage platforms. The need for decryption mechanisms to access the encrypted data also incurs addition time and costs leading to delayed and expensive diagnosis of health records. Advance researches find potential in utilizing a newly deployed security mechanism called blockchain which is essentially a distributed data storage technique able to disperse data blocks among and across the nodes in the computing infrastructure, to address these security issues of Healthcare data. Entire dataset is linked using timestamp of production of the data block and the hash of the previous data block. A personal data cloud exploiting the features of blockchain is capable of resolving the security and privacy issues of healthcare sector and also empowers an individual to take control of their personal medical data.

This chapter outlines the role of blockchain in fastening the healthcare research and empowering patients to control the privacy of their health data in addition to avail a secured regular health monitoring tool. The chapter also deals with fundamental challenges, issues of blockchain, and research outset of blockchain in the field of the healthcare information security.

14.1 Introduction

Healthcare data and services are steadily being repositioned to the comfort of convenient access and cost-effective data management offered by cloud infrastructures. Traditional cryptographic methods and other security techniques do not take care of data privacy and data security (access control) issues appropriately on cloud driven computing platforms. Beside these other concerning issues that are prevalent in Healthcare industry are long listing viz. incomplete patient records, difficulty in access at the point of care and at the patient's end, complex or incompatible exchange between different healthcare systems, restrictions on share and use of medical data due to sharing regulations, privacy liabilities, and associated financial threats because of potential leakage of private data to name a few. Certain standardized data formats can tackle few of these issues to a certain extent but still interoperability in context of exchange of medical data among various healthcare systems cannot be achieved because of lack of trust and compatible data formats of medical records. Healthcare also faces issue of the data being usable on isolated systems only, and delayed communication of these data because the data recorded for medical purpose are dispersed among all of its stakeholders. Blockchain is capable of offering a secure and private, quick, and complete access to such data which are stored on distributed storage. Healthcare information systems and software applications lack in their ability to exchange medical records across the systems and applications seamlessly.

This poses significant restrictions on smooth communication, exchange, and use of health-related records for both the patients and the care takers. However, sharing of such data without restriction is vital for effective cure delivery and quality repository of such health records. The hurdle does not come because of lack

of incompatible data formats and cross-platform systems only. The ease in sharing is also hampered due to lack of trust between different care providers, privacy concerns of individuals, data integrity breaches, threats of financial frauds and data sharing regulations too. Allowing medical information systems to share the data within and across the organizational boundaries can significantly improve the healthcare for concerned individuals. Data interoperability between providers, individuals consent to share their details, and flexible regulations can liberate the existing healthcare delivery mechanisms to become more secure, scalable without concerning much on location and trust of healthcare providers [13]. Effective care decisions and collaborative speedy treatments can be easily deployed for the patients if all these issues can be sorted out by some trusted means. An easy and breach free data exchange can also lead to preventing inadequate data gathering, improved diagnostic accuracy and flawless cure plan and medication for patients. Current practices require the patient's data to be collected and shared via paper reports which make recording and exchanging medical records ineffective because of time-consuming process of data recording, delayed preparation and delivery of health reports. The delayed health reports are sometimes useless in case of critical health issues. Since these reports are physically transmitted by the patients to various care points it is also prone to theft, lost, and damage of data copies. A consolidated and comprehensive data about all the medical history of the patient and health services availed by the patient also becomes very hard to track. Above all of it, all the data storage or processing units are healthcare provider centric and hence the patients have no control on access and use of their own medical data which is an obvious example of breach of health record's confidentiality, integrity, and availability. So there is an urgent need of technology like blockchain which is capable of defining a consistent data exchange format and easy interpretation of exchanged data with additional security, privacy, and ease of access. Because it is necessary to for patient to take control of when and to whom their healthcare data are shared and to choose what pieces of critical or noncritical health information they would be willing to share [14–20]. Existing healthcare systems does not allow patients to grant, revoke, or modify the access to their health data. Moreover, once cared for a patient healthcare provider is likely to have sensitive personal and health data of the patient permanently forever and hence putting their data to the risk of misuse. However, these providers may face financial and legal consequences when data privacy is breached but getting access to patients own historical records from these providers for having a second opinion or alternative treatment is still not easily accomplished. In addition few data formats which are rich source of critical health information are so condensed and voluminous in nature that sharing them across the organizational boundaries needs addition effort in computing and puts a significant overload on transmission bandwidth and consequently raises serious scalability concerns.

Blockchain technology is likely to become the future technology which will effectively address most of the protection issues of healthcare data stored on the cloud. Blockchain technology has the potential adaptability for various segments of healthcare industry including user-specific medical research, prevention of drug forgery, and healthcare data management but not limited to. Initially inception for

financial sector, the blockchain illustrates considerable potential of incorporating its abilities into healthcare sector.

Blockchain technology can effectively help eliminating the dependencies on a centralized data management entity to certify the source, authorship, and integrity of the information. It can also leverage security and anonymity while mediating exchange of crucial digital information and maintains an agreement on exchange policies between interacting sites. To distributed data transaction systems blockchain design inherently offers transaction immutability, transparency, and most importantly the decentralization of transaction authority which makes it secure by default. This chapter explores the role of blockchain in preserving the privacy of healthcare information and their seamless exchange between various parties without worrying about the security issues.

This chapter is further arranged in the following sections: Section 14.2 explains and illustrates the working of blockchain technology; Section 14.3 gives an overview of a general architecture of the blockchain-based healthcare data management systems. It also talks about the complexities and components of a more realistic practical architecture deployed for healthcare data management and the parameters which are suitable to assess the architectural design of healthcare systems based on blockchain; Section 14.4 raises the challenges and issues of incorporating blockchain and how it affects the privacy and integrity of health data; Section 14.5 explores the possibilities of any further enhancement to the Bitcoin blockchain to tighten the security needs of the sensitive healthcare and personal records; Section 14.6 enlists the potential applications of blockchain technology in the field of healthcare industry and its subdomains. The subsequent Section 14.7 delves deep into the prospective research directions on potential use of blockchain for the betterment and effectiveness of healthcare industry.

14.2 Blockchain: how it works?

Originally, instigated for crypto currency (the Bitcoin) in order to establish a decentralized electronic currency, the blockchain refers to a fault-tolerant distributed database which uses replicated servers to coordinate clients' interactions. Atomic transactions in such databases are broken down into blocks whose integrity is assured by hash coded links between two consecutive blocks. These hash coded links also ensure that the transaction logs of the database are impervious to any internal or external interference. As a distributed database the blockchain maintains an ever-growing list of records composed of blocks and locked together using specific cryptographic algorithms to maintain the privacy, integrity, and consistency of the data. A blockchain is maintained by a shared companion system of clients who collectively adhere to agreed rules for accepting new blocks. Each record in the block contains a timestamp or signature and an encrypted connection to a previous block in chain. If a blockchain database transaction is made from one site to another the information related to this transaction is shared among all the other companion sites. The transaction details like ownership, transaction value,

etc., are put into a block of information and a timestamp is marked. This block is then added to the existing chain of blocks. Simultaneously all the other percipient sites validate and confirm the transaction to be added to the blockchain. By such a design principle of working blockchain ensures the complete immutability of the information contained in the blocks and hence all the previous transactions at any instant of time is not only transparent but extremely difficult to be tampered. In addition to the security, trust, decentralization, and immutable transactions the blockchain technology also offers unanimity using the concept of game theory and cryptography for the transactions to be accepted by all the computing sites involved in the transaction [1]. The working of a blockchain is dependent on long-existing security and computing principles like private key cryptography, authentication mechanisms, distributed computing, etc. Combined features of these standard and popular technologies equip blockchain with remarkable security features. Figure 14.1 shows the working of blockchain.

Analogous to private key cryptography blockchain also uses a secret private key as a tool to complement an encryption algorithm to scramble and unscramble the reference of a secure digital identity while all the transactions are made public on the network. This is exactly the same as in private key cryptography that keeps the key secret but algorithm for encryption and decryption public. Secondly, using

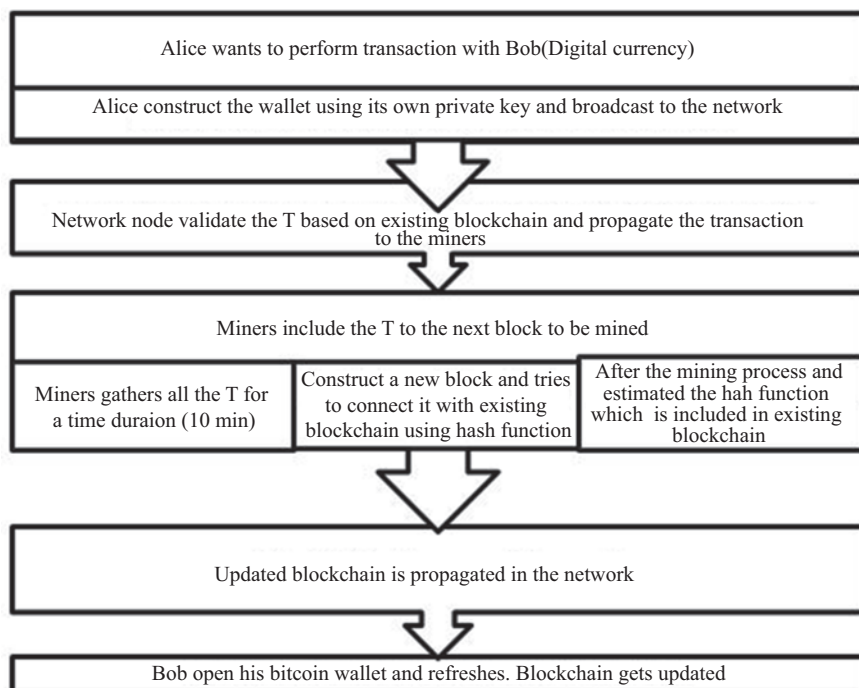


Figure 14.1 How blockchain works?

the principles of distributed computing a distributed database which shared among all the participants and any transaction update is governed by the consensus algorithms. In such distributed database storage, the database is updated in real time and no central authority is held responsible to maintain the database. Instead, participants keep the database updated. Any changes made in the database are reflected within seconds to all the concerned parties. In a blockchain environment, every one of the exchanges or transactions is verified before getting added to the blockchain. This procedure happens through calculations that approve and check every one of the exchanges or transactions. When the data are scrambled and the identity carefully marked and stored, the credibility of transaction is fixed.

14.3 The general architecture of blockchain integrated healthcare data management system

This section gives an overview of a general architecture of the blockchain-based healthcare data management systems. It also talks about the complexities and components of a more realistic practical architecture deployed for healthcare data management and the parameters which are suitable to assess the architectural design of healthcare systems based on blockchain.

The architecture presented here will serve as a reliable infrastructure for effective and undoubtedly secure healthcare information exchange [21–27]. A general conceptual architectural setup of blockchain integrated healthcare data management system is composed of a blockchain storage which will be connected to defragmented health record databases which may entirely differ of data formats and the standards of data records. Every such data storage connected will provide a secure data channel or interface to the blockchain storage to enable the seamless data sharing between these databases. A simple secret key based or a smart contract-based mechanism is then clubbed to control the transactions between these systems which are governed by suitable consensus algorithms or computations. Such mechanism plays an important role in ensuring tamper-proof recording of all the transactions and immutable logs. Figure 14.2 show the general architecture of blockchain. This simple conceptual architecture can be depicted as follows.

In practice, no such simple architectures are deployed. However, this simple general architecture itself is a result of continuous evolution in initial healthcare systems architectures but the real scenarios may consist of a more robust architecture with complex design components than that of illustrated here in figure above. One of such advanced architecture for e-health system was presented through advanced Block-Chain(ABC) approach which is aimed to meet the current requirements of the healthcare industry and can also serve as the foundation for the next generation architectural improvements in the field [2]. The design of such architecture has evolved from the sheer need of an interoperable and scalable data exchange platform which can cater the needs of flexible data representation and efficient healthcare services. Such advanced architectures can also tackle the intercommunication or integration of clinical, financial, or other institutions involved simultaneously which

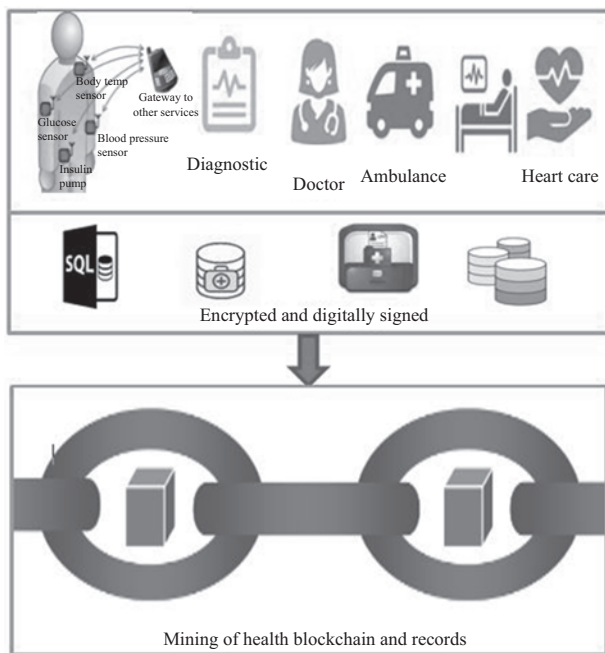


Figure 14.2 General architecture

is normally missing in the case of simple health record systems like electronic health records (EMRs) systems. Advance architectures can ensure the optimization of data access and usage accountability and can perfectly balance it with the regulatory norms for privacy and security of patient's sensitive personal data. Previous evolutions in the architecture was result of improvements in the features which contributed to cross organizational boundary or network interoperability, data security mechanisms, enhancement of computing platforms, and the rise of effective and faster software development frameworks. In addition to the scalable and globally interoperable health information systems which was capable of dealing with multiple origin and formats of voluminous data, advanced data processing need was also a key factor to such design complex design evolutions. Every advancement in the architecture of the health information system was aimed to control and maintain data integrity, determination of its origin, security, privacy, completeness and reliability in order to offer a faithful patient identification, authentication, and access control applications for the healthcare industry. Figure 14.3 depicts the architecture of healthcare blockchain.

The advanced blockchain architecture for healthcare defines any transaction as an event of generating, submitting or exchange of data which is common across all the previous health information systems too. Electronic health records, clinical observations, diagnosis reports, billing information, treatment plans, prescriptions, insurance information, and payments are a few examples of transactions. This

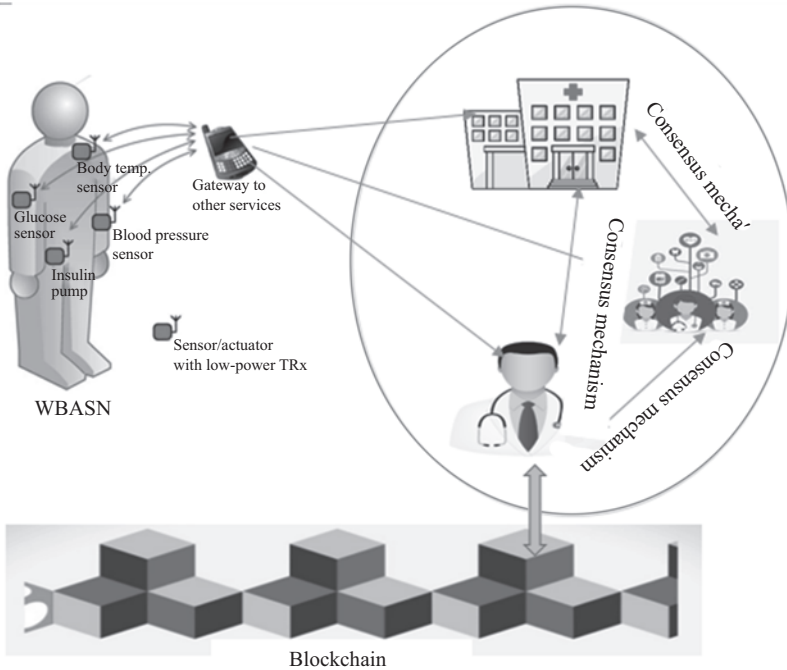


Figure 14.3 Architecture of healthcare blockchain

architecture stores all kind of transactions in the form of blocks, each linking to the previous one and the next block like a chain. Figure 14.4 shows the key features of blockchain.

Each participant on the blockchain has access to all the transaction records all the time and no one having the central authority on the stored transactions. Such architecture aids to transparency to the system. Communication between the parties can happen directly without any need of central governing authority to control the transaction and resolve the transaction disputes. However, each party is allowed to act independently but the transaction is recorded on the blockchain storage only after a validation via predefined agreement protocol of the blockchain. Domain-specific records can also be stored out of the blockchain to facilitate the distribution of the storage. This architecture is highly distributed and fault tolerant in nature and inherently immune to transaction modification or duplicity. All the transactions are assured to be chronological and persistent once they are stored on the chain and no one is allowed to alter as they are linked to all the previously stored transactions. Transactions can be triggered via algorithms of choice and embedded procedures can also be deployed for security and regulatory norms, and reporting of various transactions.

The core metrics for assessment of any such decentralized conceptual or practically deployed blockchain-based solution constitutes of the compliance to protect

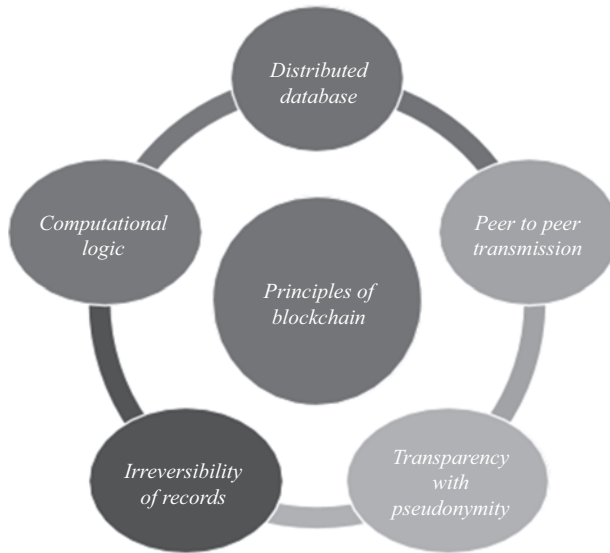


Figure 14.4 Key features of blockchain

against confidentiality breach, adherence to the Turing completeness theory, structural and contextual interoperability, solid patients identification and authentication support, communication scalability in context of large number of simultaneous users, and their ability to empower the patients to control access to their data.

1. A central perception of secure health information system is to must be secured against privacy breach or in another word it can be said that an essential future of healthcare systems is to protect the user's data against any confidentiality breach. Specifically, the end-to-end healthcare service delivery and the exchange of data during this delivery must be secured. Indeed at all the stages of data flow whether it is the data generation, processing, sharing to care provider, and storage of the data has to ensure the confidentiality of the user's information. Current practices bring various information security mechanisms like encoding and firewall technologies to ensure this. At the point when utilizing a blockchain where all data are freely accessible, in any case, it is non-insignificant to safely oversee as well as store delicate information. For instance, putting away encoded health data on the blockchain is illogical for the accompanying reasons:
 - Significant storage capacity cost and computational overhead would be inescapable to keep up and recover the encoded information stored on blockchain.
 - Any information composed into the blockchain will remain publically accessible until the blockchain itself is erased.

Additionally, if the encryption component used to secure information on the blockchain is broken, either by advanced computation or algorithms, the information privacy would be at stake irrespective of whether encryptions techniques are updated frequently to give most extreme assurance to protect the confidentiality. Any such breach will land the patents into financial adversary or the care providers or information providers to legal consequences. A well architecture blockchain-based decentralized health system should confine the capacity of encoded information storage on the blockchain. For example, it might store some no decodable storage address to access to genuine patient data. Similarly, it might store just the minimal information required to retrieve or transact sensitive information through a secure channel which permits an agreement on the blockchain to search or access information sources outside the blockchain while guaranteeing they are certified and unhampered.

2. Few blockchain technologies serve for a solitary reason like financial exchange only. For example, Bitcoin [1] is planned as a cryptographic money, that is, used to purchase and sell products on a commercial center safely and pseudo-namelessly. These blockchain however popular for financial exchange are not intended to trade differently organized information models, which are at the core of healthcare industry. Healthcare has diverse data-models to deal with. An interoperable health information system should fairly deal with the exchange of sensitive patient data. It ought to encourage interchanges of these diverse data among different stakeholders of the industry too. To devise structure cutting edge healthcare application architecture, consequently, the fundamental blockchain technology should be Turing complete, that is, it ought to contain programming or computing capabilities equipped for illuminating any calculation issue. For example, Ethereum is an open-source blockchain technology with a smart contract that underpins the Turing completeness into it. It would thus be able to be utilized for a wide range of activities significant for healthcare decentralized applications including healthcare data access control and exchange [3].
3. Two kinds of participants in healthcare industry require specific identification and authentication to access and use the data. The first kind of participants is patients and the other is medicinal services experts like practitioners, doctors, insurance agents, healthcare centers, pharmacists, and lab technicians. Both of these group's unique requirement for their identifications and authentication is based on the inherently different nature of their access privileges to the healthcare system data and other useful resources. One the one hand there are essentially a greater number of patients than medicinal services experts and on the other hand health services experts have less demanding access to health-related information. Since the number of patients is significantly large it is inevitable to forget or misplace a patient's identity. A well-designed healthcare information system must address this issue with utmost care to prevent redundant data recording and repeated clinical trials and diagnosis. It should also be able to incorporate a full proof methodology to validate the access rights of the patients before retrieval of the forgotten identity. The identification mechanism should be

such that it uniquely identifies the patients even in the event of the loss of identity and still keeping his identity anonymous on the blockchain storage using a suitable way to reallocate the identity and existing data to that user.

4. The vendor-specific data models, their diverse data formats make these data difficult to exchange across the applications and organizations. A well architecture healthcare system should remove all these limitations and should provide a platform for easy integration of diverging data models into a unified and universally acceptable model to offer contextual interoperability of the healthcare information systems which will consequently empower the exchange and interpretation of clinical information irrespective of their original data models. To abstain from presenting extra multifaceted nature caused by diverse information models utilized inside these blockchain-based decentralized applications, it ought to align its operations for various data models and data standards.
5. Since healthcare information systems services may need to administer for a large number of clients it must be scalable to handle the communication overhead to and fro the blockchain. Such ability is one of the key design assessment factors among other metrics. It should also able to diminish the communication gap between different stakeholders of the systems. One another critical assessment parameter for decentralized blockchain-based health information system is in its attainability of low cost, low computational overhead operations in addition to minimizing the traffic on the blockchain. A well design system will take care of the quality of data that are recorded on blockchain and also will enhance the systems interoperability in all aspects while scaling the system or users up or down.
6. Last but not the least blockchain-based healthcare systems must give the patients easier access to and control over their data to enable patients' centric healthcare services. Such system will also empower the patients to generate their health reports their own, to take part in the treatment decision for them, to take second opinion or to consult care provider of their choice, etc. A healthcare system which will have all or some of these aforementioned qualities will be said to have a well-designed conceptual or realistic architecture.

14.4 Privacy and integrity of healthcare data: challenges and issues of utilizing blockchain

While it appears so fascinating to utilize the inherent properties of blockchain to address variety of issues of healthcare data it is also essential to understand the major challenges that this technology can face when incorporated into existing healthcare data management systems. This section explores a few fundamental challenges face by blockchain-based distributed and decentralized applications. These challenges are mostly related to design improvements, data storage requirements on blockchain, protection of patient's data privacy, and communication scalability of such blockchain-based systems.

14.4.1 Design improvements

Blockchain is secure as the transactions are immutable but it should support the architectural upgrade in the existing healthcare system with ease and at the same time the complexities for integrating blockchain technology to the various healthcare systems should be minimal. In blockchain-based decentralized applications transactions logs are hard to change and even change is also recorded as immutable logs but the blockchain technology in healthcare system should ensure that there exists a scope of change in data structures (mainly defined using smart contracts). Data formats may and this change has to be reflected easily providing a chance to systems to evolve and upgrade. That is why it is essential to design the necessary data structures in such a way that it is loosely coupled with its logical counterparts and will minimize the impact of any such change. A new contract object is created on the blockchain if the smart contract is altered. Change record being immutable it becomes mandatory to take all the design decisions made in advance before creating the smart contract in order to reduce the overheads induced by these design modification.

14.4.2 Data storage requirements

Healthcare is the most data-intensive domain. Even widely popular social networks and multimedia sharing platforms cannot produce this data. But current practices make it hard to capture the data into healthcare systems from the traditional paper form as most of data generated by biomedical imaging, laboratory testing, doctor's prescriptions, and diagnoses reports recorded on papers only [4]. Besides patients clinical records Healthcare industry also obtains data from care providers and billing agents, insurance companies, and other stakeholders. This makes health data costly to data entry, archive, and access as and when required which may obviously incur enormous storage overhead if stored in a blockchain setup. Data errors and volume can be handled a bit if normalization techniques are wisely put under action but it can encounter data access failures due to restriction put on data size limit (incorporated to prevent cyber-attacks by simulating infinite looping of data operations) by blockchain environment. So minimization of data storage requirements on the blockchain becomes a crucial aspect which cannot be ignored.

14.4.3 Data privacy and protection

To aid to the interoperability of the blockchain-based systems identification and authorization of the participant's involved and secure storage and exchange of the data and access control on data sources and data users must be ensured. Blockchain has emerged as solution to few of these challenges due to their inherent working principle but still there are few risks because of transparency of data transactions. Each participant of the blockchain transaction has a complete copy of the transaction ledger which is updated and properly notified if anyone in the network has done the transaction. However secure cryptographic approaches are deployed but still it gives an opportunity in peer-to-peer network of users to breach with these encryptions. Thus the private data of the patient is at risk of being compromised.

14.4.4 Communication scalability-based healthcare systems

As the healthcare deals with reasonably massive number of patients' data, any blockchain-based healthcare data management system should be capable of detecting and tracking any changes which are relevant for data update or health service need in real time manner and obviously for all the participants. Otherwise the timely exchange of health information and the quality delivery of healthcare services can never be achieved. A blockchain-based healthcare ecosystem which is not scalable to the huge number of patients and variety of the data formats will never help the industry to review and act upon the demand of patients.

14.5 Healthcare data management: scope for tightening security offered by blockchain

Healthcare data are a perfect blend of personal and sensitive information which can attract cybercriminals for taking financial benefits from the illegal access to these data. These data may also be able to be insightful for some health insurance providers to figure out uninsurable patients by analyzing their genetic order if any from their medical data. It means a lot use and misuse can be financially profitable for different stakeholders of healthcare industry [5]. Use and access to data to improve the effectiveness is fine but the need for privacy and securing these data by preventing any such unauthorized access to the data becomes crucial to mitigate the impact of financial or legal consequences. Access control mechanism and regulatory policies can effectively reduce the external access to the data but are ineffective against the insider attacks. Recently introduced Bitcoin blockchain comes to rescue too many of such issues to protect and keep the privacy intact. After its successful incorporation in Bitcoin, blockchain was sought as a secure healthcare data management tool. It gave the way to a decentralized and distributed database in the form of a specialized data structure called blocks which were interlinked to in the order of time stamped truncation and hence named blockchain. These blocks are distributed across the infrastructures and no central authority is there to control and resolve the transaction and transaction disputes, respectively. Each block is marked with its timestamp of production and cryptographic hash of the previous block and the content and origin of the transaction. This way the healthcare data and data collecting point's information can be recorded. The detailed working of the blockchain technology has already been described in Section 14.2. However this blockchain offered data integrity and distributed storage and access may possibilities for healthcare industry but the same features poses many significant problems too. The strong integrity of the blockchain data makes the transactions immutable but it ends the scope of any modification or correction once stored on the blockchain. However such modification or complete erase of the healthcare record may be requested to protect the privacy of individuals at times which can be troublesome as the transactions are interweaved. An enhancement to blockchain database is a smart contract which was first incorporated in Ethereum blockchain.

Data privacy ensure that the persons keep control over access to the data. Due to the privacy breaches, the patient and healthcare providers can erode the trust in the system. Most of the healthcare providers break up the privacy of patient's data by providing it to the third party. Internet of things (IoT) play significant role in healthcare system without any human involvement. Modern healthcare system architecture consists of body sensor network (BSN) which continuously monitors the patient and transmits the information to the remote healthcare professionals or remote cloud based server. The challenges of designing an efficient healthcare architecture is to transfer the sensitive data efficiently, securely, aggregating and indexing a large streams of uninterrupted data while preserving privacy. The blockchain technology of a digital currency is not suitable for IoT healthcare system. The security algorithms which used in digital crypto currency have high computation cost, more delay, and processing times.

The main key features and its challenges of e-healthcare architecture [6] and blockchain component for distributed storage of data are as follows:

1. **Fast storage and access:** The body area sensor networks generates a huge volume of data which need to be processed rapidly in order to provide quick response for some diseases. Generally, sensor nodes are limited in an energy, processing, communication range, storage, and computation. The sensor nodes have a great challenges to perform computation processing and storage resources. The data which generated from the patient's body sensors are not necessary to be a sensitive data to store.
2. **Authentication of users:** To prevent the attacker to intercepting the flow of data, the authentication of user is must. Authenticated node only can participate in the data transfer. Even though the symmetric and asymmetric algorithms are used to provide confidentiality of the data which cannot be decrypted without using the key. In asymmetric cryptography algorithm uses a trusted third party to serve the public and private key pairs. The dependencies of trusted third party lead to security pitfall, stop monitoring the real-time patient's data, fault tolerance, and create bottleneck problems in IoT settings. The asymmetric key cryptography algorithms have more complex computation as compared to the symmetric key algorithm. Most of the healthcare architecture system uses a symmetric key algorithm to generate a key between the BSN and patient-centric agent; asymmetric algorithm and blockchain are used to secure sensor data provider and database.
3. **Role-based access:** Role-based access control discusses the delimited rights of healthcare experts on patient's data according to the proficiency. The healthcare information contains the sensitive information about patient's health; patients can allow to restrict the access based on role.

Thus, it can be seen that blockchain provides more opportunities' to the healthcare providers, cooperate to manage the health data, and participate in a transaction. Blockchain has unique competence to update the transaction automatically and audit log instantly. For the healthcare data transaction, the blockchain provides the extension of distributed database and cost-effective as compared to the

existing methodology. The concept of the distributed ledger based on the idea of mutual consensus and trust helps to reduce some of the challenges such as complex administrative transaction, security, and privacy of the healthcare data when it is shared between different organizations. The distributed ledger provides more level of accuracy, privacy, more robust integrity while providing more control over their data and security for stakeholders. The distributed ledger is initially used in the financial application. Gradually, the concept of blockchain applied to different sectors such as smart contracts, healthcare, industrial, governance, etc. One of the exciting and extended applications of blockchain is a smart contract. The smart contract provides an efficient, cheaper, and faster way of executing the contract in a decentralized way. Some of the smart contract platforms are Ethereum, rootstock, Hyperledger, ripple, and Quorum.

14.5.1 Technical advancement in the fundamental principles of blockchain

14.5.1.1 Consensus model

A blockchain comprises a large number of nodes; each node holds a public ledger which consists of a large number of transaction data called blocks. Each block is linked with preceding block using a hash function which forms a chain of blocks. Whenever the new transaction enters into a network, the transaction is validated with the help of the consensus model. One of the primary significant challenges of blockchain is in what way to ensure that the data held by every node of the distributed network are same. Therefore, it needs consensus algorithms to ensure the consistent data/state of transaction among the nodes. Some of the consensus models are Proof of work (PoW), Byzantine fault tolerance, Proof of Stake (PoS), Proof of Authority (PoA), ripple, and tender mint.

14.5.1.2 Authentication

For the healthcare applications, two important parameters need to be considered such as verification and authentication of user's information. The blockchain technology needs to verify a patient's identity, health information or prescription history. The identity of patients is recognized using a public and private key pair. The private key is kept secret and only known to the user, and the public key is shared with others on a blockchain. The person who initiates the transaction must sign using the private key. The digital signature is used to verify the authenticity of the transaction.

14.5.1.3 Distributed consensus-based on network scenario

The permission and permissionless network can differentiate the identity of the user in a network [7]. In permissionless network, any node can join the network at any time without revealing its identity. Examples of the permissionless network are bitcoin, Ethereum, etc. The permission mode is also known as a private model; in which identity provider controls the identity of the user. Example of permission model is Hyperledger.

14.5.2 *Ethereum*

Ethereum is permissionless blockchain and open. Generally, Ethereum means World Computer platform which provides users to run distributed applications in a noncentralized way. Ethereum is open which available anywhere and at any time.

It is mainly developed for smart contracts and advances the concepts of scripting, and it also allows the users to develop their random consensus-based applications, own rules for ownership, a format of transactions, and transition functions. It provides a simplified two line program codes for Namecoin.

14.5.2.1 **Ethereum architecture**

The smart contract is also known as Decentralized application which runs on Ethereum Virtual machine (EVM). Ethereum can run in public as well as private networks. Ether is an innate crypto currency of Ethereum. Figure 14.5 shows the architecture of Ethereum. Each Ethereum node runs on Ethereum virtual machine. The mining process depends on PoW. Whenever the node receives a block, the EVM runs all the transaction on specified in the blocks. The client can communicate to the EVM using SDK.

Each transaction has a particular format which has two address. Ethereum performs two different functions such as transfer the value and execution. The consensus is carried out through the Proof of Work (PoW) [4] which is similar to the bitcoin. Figure 14.5 shows the Ethereum architecture.

14.5.2.2 **Ethereum account**

The state of Ethereum is made up of objects called accounts. Ether balance plays significant role which is used to pay the transaction fees in Ethereum. Ethereum consists of two types of account such as externally controlled account and contract

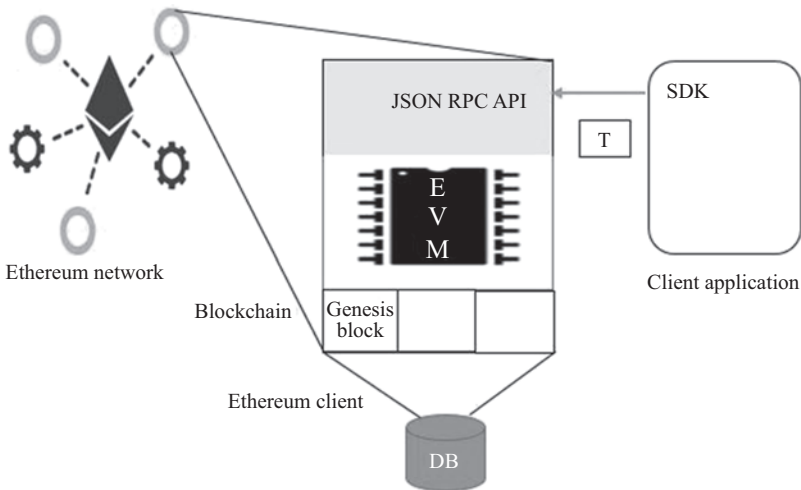


Figure 14.5 Ethereum architecture

account. In this externally controlled account, the user can perform transaction (transfer data) from one account to another Ethereum account by generating and digitally signed using the private key just like a bitcoin. It is under the control of private key which does not have code. The contract account is for smart contracts which is controlled by the contract code. Each smart contract has contract account. To read and write the storage and to create a smart contract, it needs to activate the code once it receives the message. The address size of each account is 20 bytes and the information and value are transfer between the accounts. Ethereum account comprises of four parts as follows:

1. Nonce
2. Ether balance
3. Contract code
4. Storage

Message of Ethereum are alike as bitcoin, but some of the difference between Ethereum message and bitcoin are as follows: in Ethereum, the message can be generated by externally controlled account or smart contract account but in bitcoin it is generated externally, the explicit option is available for Ethereum message, and Ethereum message received by smart contracts have concept of function which return a response for recipient of message. Figure 14.6 depicts the transaction block of Ethereum.

Transaction in Ethereum refers to the digitally signed data transferred from an externally controlled account. Transaction contains the following data such as receiver address, signature, sender identity, ether balance, data needs to send, STARTGAS, and GASPRICE. In order to limit the endless number of loops in the code, STARTGAS is used to restrict the number of computational steps of code executing during an execution. STARTGAS is used to limit the infinite number of loop in the code. GASPRICE is a miner fee to pay for computational step. For each computational step, the GASPRICE is the payment to pay for miner. If the transaction is run out of the gas means all the state are reverted. The transaction fee is calculated by means of multiplying the STARTGAS and GASPRICE and the sending account address found from the digital signature. Subtract the transaction fees from the

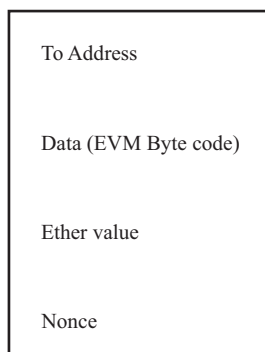


Figure 14.6 Ethereum transaction block

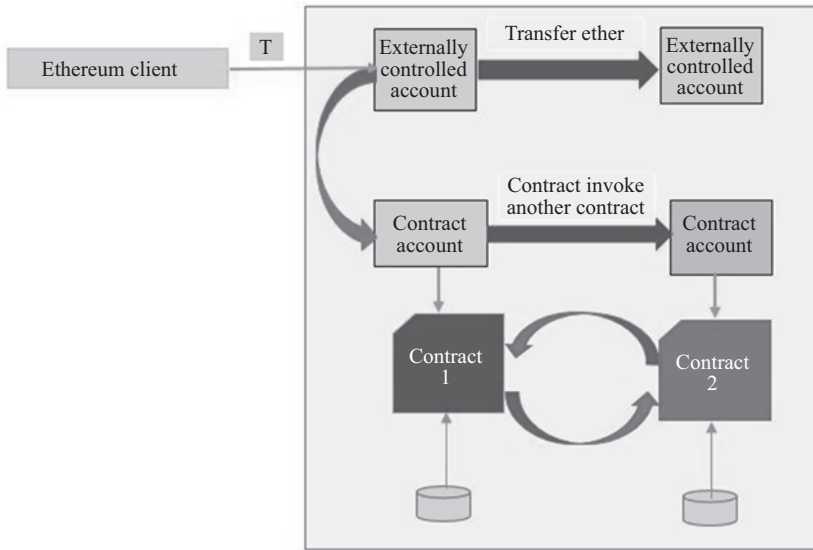


Figure 14.7 Ethereum account

senders account and increase the nonce value by 1. If there is no money in the account then returns error message. The hash function and nonce are used to calculate the address of the contract. Figure 14.7 shows the Ethereum account.

14.5.3 Hyperledger

Hyperledger is an open source permissioned blockchain initiated by Linux foundation. The three categories of Hyperledger services are as follows: Membership services, blockchain, and oraclize chain code services. The membership services provide identity of the user, privacy, and confidentiality of the network. The modular architecture of Hyperledger deals with different consensus algorithm and state machine replication algorithm. Hyperledger fabric is a private blockchain which allows the authorized user only to access and to be the part of ecosystem. The practical Byzantine fault tolerance mechanism is used to offers transparency and governance for all the participants in the blockchain system to avoid malicious parties from the network.

For the application of healthcare system, the permissioned Hyperledger allows the authorized person to access the data from the network. It provides proper sharing of data, high level of security, and protect against the attacks as compared to the enterprise system. Table 14.1 shows the assessment of Ethereum and Hyperledger.

14.6 Potential uses of blockchain technology in healthcare industry

This section enlists the potential applications of blockchain technology in the field of healthcare industry and its subdomains based on features offered by blockchain.

Table 14.1 Assessment of Ethereum and Hyperledger

Protocol	Speed of transaction	Access	Program	Crypto currency	Governance	Automation
Ethereum	$\cong 15$ per seconds	Either permissionless or permissioned	All participants can see and follow the all transaction and update program in real-time	Ether	Enforced and coded by smart contract	Smart contract allows program automation when specific condition met
Hyperledger	$\cong 160$ per seconds	Private Blockchain	Only authenticated participants can access the shared ledger	Faster transaction and throughput		It allows automation inside the supply chain process at standard

14.6.1 Prescription and supply tracking of narcotics drugs

Being decentralized and auditable by design the blockchain technology can easily distribute the knowledge that some transaction has happened with or without sharing the content of the transaction to various regulatory authorities, patients, and the healthcare providers. This feature of the blockchain can be exploited to track the prescription of narcotics used in order to short term relief from the pain to the patients which can cause them temporary or permanent addiction to the prescribed drugs. Since it can be tracked it can be easily regulated too. The same feature can also help to track the purchase of such narcotics by registered practitioners and doctors and sells of these harmful narcotics by pharmacists leading to an effective supply chain management and regulation of frequent use of these drugs for anesthesia and pain relief at the cost of patient's addiction.

14.6.2 Flexible data exchange between parties

A vast variety of equipment's for measuring health vitals can be easily integrated to daily use gadgets like smartphones and decentralized applications which are developed based on blockchain technology. These records not only can be stored on the capturing devices but also be shared to anyone as and when required. By this decentralized authority approach patients can be empowered for direct transactions of their critical and sensitive data to healthcare provider of their choice and can also take leverage of controlling the access to their data and benefits out of it. Here blockchain can also bridge the gap of cross-organizational data sharing barriers if incorporated appropriately to existing healthcare systems and adheres the standard clinical data formats recommended for health data transactions.

14.6.3 Patient controlled healthcare services

Despite being the most important participant of healthcare industry services the patients remain disengaged in various treatment-related decision making which

degrades the quality of treatments and also makes the treatment costly because most of the time healthcare services are deliberately imposed on patients. Blockchain can enable patients to take control of their data and hence leveraging them to reach out for second opinion from different care providers. Switching to different providers with all the historical medical reports viz. visit records, medicine recommendation, previous diagnoses reports, treatments given, etc. will surely become easier for the patients, saving them their time and physical efforts, money, and most importantly will enable them to take decisions regarding their need for healthcare services [8]. Blockchain permits distribution of control via decentralization backed up by consensus algorithms. Patient can easily get consolidated medical history reports by combining test profiles recorded at different care points using such data distribution services offered by blockchain technology. Such services set up with smart contracts also guarantee that patient never misses the control on their data access and are fully aware of the data source. In addition they are informed if someone has accessed their data. Thus, data sources and access are made transparent to patients through tamper-free transaction logs.

14.6.4 Learning ecosystem development for decision making

Blockchain not only can be a leverage to expedite information sharing but also can prevent redundant clinical records to be recorded in distributed data storage. With this rich quality data collected from huge number of patients, artificial intelligence can be deployed to construct predictive models which can greatly assist in making care and treatment decisions much before the actual treatment plan is followed. An addition learning ecosystems can also be designed by implementing and deploying blockchain technology to exchange these predictive models to improve the accuracy of medical insights fetched from different similar models.

14.6.5 Digital identification of the patient

Blockchain technology is sufficiently eligible for creating a unique and flawless patient identification system which is at the core of any health information exchange. Such patient identification is based on the unique pattern matching in the patient database. A certain set of data features are found only in any specific patient record which makes it possible to identify the patient. Such kind of systems if deployed can address the issues of duplicate, incorrect, and incomplete data records of the patients in addition to providing a full proof patient identity matching. The deaths due to such identity and prescription mismatch can be addressed with the help of proof of ownership concept of blockchain which is well weaved in its design itself [9]. The very design of the blockchain technology is capable of incorporating a decentralized unified patient identity system. To represent identity blockchain technology uses hash secured address. And each such address is further linked with a unique key to verify the authorship of the transaction. Blockchain can enforce standard verifiable identity for patients who can be sharable across the healthcare facilities and political boundaries. Reassignment of unique key and address can also be done easily to cope with the loss of access to data.

14.6.6 Insurance claims reimbursements

Incomplete, incorrect, and duplicated data may lead to mismatched individual identity which in turn raises other concerns like multiple clinical data recording or diagnoses report and denied insurance claims. Having already seen the importance of blockchain technology in digital identification of patients it becomes very obvious that it can be effectively utilized in healthcare insurance claims reimbursements too. Patients normally may pay a portion or lump sum of incurred care services cost at the time of treatment but is likely to claim (if insured) a payment or refund from insurer which is liable to pay the patients in lieu of all the expenditure done for minor or major medical emergencies, accidents, treatment of diseases, or even for a normal routine checkup. The healthcare provider or the patients directly are reimbursed through the claims whereby the insurer determines, validates, and confirms their financial responsibility against that claims.

These payments are done only if the claim information is correct in all respects. Even a small spelling error in the name can give the insurer a chance to decline the payment. Other reasons for claim rejections may include lack of proof of supporting the service cost incurred or incomplete or incorrect details of the patients [10,11]. Blockchain comes to rescue again as the smart contract used in it gives transparent way to exchange the information between patients, insurer, and the healthcare providers without any delay and minimizing any chance of fraud claims. Also any correction, if needed, can be done in timely fashion. Blockchain smart contract keep all the involved participants appropriately notified and updated.

14.7 Future research directions of utilizing blockchain in healthcare

Inherent complexities of the healthcare domain open a wider opportunity for research arena in which blockchain can find its potential use in developing information rich and responsive healthcare information systems. A deep diving research on creating an interoperable, easily linkable blockchain healthcare system architecture will definitely be a significant area to work on without any doubt which can lead to overcome many challenges of utilizing blockchain in healthcare industry. Architectural research and design [6,12] emerged out of it will help eliminate the issues of data storage, exchange, and scalable transaction communication as most of the initial architecture are not able to cope these problems with ease. On a more technically sound ground an architecture which can balance between simple practical design to achieve interoperability and still addressing the critical security and confidentiality concerns should be the aim of upcoming researches. Extensive researches to aid on secure and effective blockchain technology-based software application development practice are also open in addition to the above stated prospective architectural evolution.

Fundamental researches which can educate the domain experts and developers on mitigating the limitations of existing blockchain technology are also in scope. Approaches to certain the quality and efficacy of blockchain-based architecture must also be put on track so that the systems can be tested and validated based on

various performance parameters like time and cost of computing, scalability of the communication, storage needs, and many other assessment metrics to ensure effective system deployments.

The blockchain technology in its initial form was mainly introduced to resolve the concerns of digital financial transactions. So there is an ample scope of investigation to enhance existing blockchain technology in the context of healthcare industry or to design an entirely new blockchain network that can take all the good of the existing one and additionally will serve the purpose of dealing with specific health-related service concerns of the healthcare industry. Simply saying, healthcare domain specific blockchain technology can be put on development goals.

These researches are not limited to the areas that have been listed here. A wide range of applications, design improvements, and quality concerns addressing researches can be carried too.

14.8 Summary

Blockchain with smart contracts are the pillar for designing robust decentralized systems and distributed applications which may serve a wide range of purposes to the healthcare industry. Facilitating fast and secure data exchange, managing digital identity of patients, tracking prescriptions and supply behaviors for drugs, finding medical insights to support decision making, fastening claims reimbursements, and enabling patients control on their data are few promising applications of blockchain technology to healthcare industry. Despite the very complex design of data flow in the healthcare industry the blockchain technology is capable to resolve key issues of healthcare domain including data privacy protection, application scalability, cross-boundary data exchange, and storage requirement minimization to name a few but not limited to. This chapter explored all these concerns of healthcare data and recommendations to mitigate those challenges using blockchain technology. Based on the information presented in this chapter it can be concluded that blockchain offers an interoperable data management platform using the properties of decentralization, distribution, immutability, and verifiability which was almost impossible to attain using other traditional centralized tools and platforms. This chapter depicts the great potential of blockchain technology in enhancing the current healthcare ecosystem with its unique characteristics which are inherited in it by default due to its design and working principles. Blockchain not only has a wide range of application possibilities in healthcare industry but also enormous research opportunities are there on utilizing blockchain in healthcare.

References

- [1] Amofa S., Sifah E.B., Agyekum K. O.-B O., Smahi A., Xia Q, and Jamea C., "A blockchain-based architecture framework for secure sharing of personal health data," *IEEE 20th International Conference on E-Health, Applications and Services*, Ostrava, 17–20 September, pp. 1–6, 2018.

- [2] Matthias Mettler, and M.A., "Blockchain technology in healthcare the revolution starts here," *IEEE 18th International conference on e-health networking, Applications and services*, Munich, Germany, 14–16 September 2016.
- [3] Nakamoto S., *Bitcoin : a peer to peer electronic cash system*, White Paper, 2008.
- [4] Buterin V., *A next generation smart contract and decentralized application platform*, Ethereum White Paper, 2013.
- [5] Vora J., Devmurari P., Tanwar S., Tyagi S., Kumar N., and Obaidat M.S., "Blind signatures based secured e-healthcare system," *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, July 11–13, 2018, pp. 177–181.
- [6] Azaria A., Ekblaw A., Vieira T., and Lippman A., "MedRec: using blockchain for medical data access and permission management," *Proceedings of the 2nd International Conference on Open and Big Data (OBD16)*, Vienna, Austria, 2016, pp. 25–30.
- [7] Zhang P., Walker M.A., White J., Schmidt D.C., and Lenz G., "Metrics for assessing blockchain-based healthcare decentralized apps," *19th IEEE International Conference on e-Health Networking, Applications, and Service*, Dalian, China, 12–15 October 2017.
- [8] Tanwar S., Obaidat M.S., Tyagi S., and Kumar N., "Chapter 10: Online signature-based biometrics recognition," M. S. Obaidat, I. Traore, and I. Woungang (eds.), *Biometric-Based Physical and Cybersecurity Systems*, Springer, Nature Switzerland AG, 2019, pp. 255–285.
- [9] Tanwar S., Tyagi S., Kumar N., and Obaidat M.S., "Chapter 21: Ethical, legal, and social implications of biometrics technologies," M. S. Obaidat et al. (eds.), *Biometric-Based Physical and Cyber Security Systems*, Springer, Nature Switzerland AG, 2019, pp.535–568, 2019.
- [10] Azaria A., Ekblaw A., Vieira T., and Lippman A., "MedRec: using blockchain for medical data access and permission management," *2nd International Conference on Open and Big Data*, Vienna, Austria: IEEE, 22–24 August, 2016, pp. 25–30.
- [11] Tschorsch F., and Scheuermann B., "Bitcoin and beyond: a technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, 2016, vol. 18(3), pp. 2084–2123.
- [12] Zhang J., Xue N., and Huang X., "A secure system for pervasive social network-based healthcare," *IEEE Access*, 2016, vol. 4, pp. 9239–9250.
- [13] Sadiku M.N.O., Eze K.G., and Musa S.M., "Block chain technology in healthcare," *International Journal of Advances in Scientific Research and Engineering*, 2018, vol. 4(5), pp. 154–159.
- [14] Esposito C., De Santis A., Tortora G., Chang H., and Choo K.-K.R., "Blockchain: a panacea for healthcare cloud-based data security and privacy?," *IEEE Cloud Computing*, vol. 5(1), pp. 31–37.
- [15] Rennock M.J.W., Cohn A., and Butcher J.R., "Blockchain technology and regulatory investigations," *The Journal Litigation*, March 2018.
- [16] Zhang P., Schmidt D.C., White J., and Lenz G., *Blockchain Technology Use Cases in Healthcare*.

- [17] Krawiec R.J., Barr D., Killmeyer J., Filipova M., Nesbitt A., and Israel A., "Blockchain: opportunities for health care," *Deloitte Consulting LLP Analysis*, 2016.
- [18] Mamoshina P., Ojomoko L., Yanovich Y., *et al.* "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, 2018, vol. 9(5), pp. 5665–5690.
- [19] Clauson K.A., Breeden E.A., Davidson C., and Mackey T.K., "Leveraging blockchain technology to enhance supply chain management in healthcare: an exploration of challenges and opportunities in the health supply chain," *Blockchain in Healthcare Today*, pp. 1–12, vol. 1, 2018. ISSN 2573-8240 online <https://doi.org/10.30953/bhty.v1.20>
- [20] Fernández-Alemán J.L., Señor I.C., Lozoya P.Á.O., and Toval M., "Security and privacy in electronic health records: a systematic literature review," *Journal of Biomedical Informatics*, 2013, vol. 46, pp. 54–562.
- [21] Wonga M.C., Yee K.C., and Christian N.H.R., "Socio-technical considerations for the use of blockchain technology in healthcare, Building continents of knowledge in oceans of data: the future of co-created ehealth," Ugon *et al.* (Eds.), pp. 636–640, 2018 European Federation for Medical Informatics and IOS press.
- [22] Kumari A., Tanwar S., Tyagi S., and Kumar N., "Fog computing for Healthcare 4.0 environment: opportunities and challenges," *Computers & Electrical Engineering*, vol. 72, 2018, pp. 1–13.
- [23] Vora J., Tanwar S., Verma J.P., *et al.*, "BHEEM: a blockchain-based framework for securing electronic health records," *IEEE Global Communications Conference (IEEE GLOBECOM-2018)*, Abu Dhabi, UAE, December 09–13, 2018, pp. 1–6.
- [24] Hathaliya J., Tanwar S., Tyagi S., and Kumar N., "Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach," *Computers & Electrical Engineering*, 76, pp. 398–410, 2019.
- [25] Vora J., Tanwar S., Tyagi S., Kumar N., and Rodrigues J.P.C., "FAAL: fog computing-based patient monitoring system for ambient assisted living," *IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom-2017)*, Dalian University, Dalian, China, October 12–15, 2017, pp. 1–6.
- [26] Vora J., Italiya P., Tanwar S., *et al.* "Ensuring privacy and security in e-health records," *International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*, Colmar, France, July 11–13, 2018, pp. 192–196.
- [27] Tanwar S., Thakkar K., Thakor R., and Singh P.K., "M-Tesla-based security assessment in wireless sensor network," *International Conference on Computational Intelligence and Data Science (ICCIDS 2018)*, NorthCap University, Gururgram, April 07–08, 2018.

Chapter 15

Enhancement of health-care services using blockchain with data authentication and protection

Bharat Prajapati¹ and Satyen Parikh¹

15.1 Introduction

Historical details of a patient always leave a very critical challenge for treatment in health-care industry. As the population is exponentially growing across the world, people may need to consult multiple places for their treatment or consultation with different health-care professionals. Doctors also require performing various medical tests to know the current health status. So a secure platform is required, on which patients' data can be shared among the authorized people with necessary details only. The platform must have a compatibility of sharing medical records in a secure way. However, people are more interested in dealing with medical organizations which give assurances to maintain full privacy about health treatment. In this context, blockchain is one of the upcoming technologies that ensure the requirement of secure data sharing.

One interesting, powerful feature of the blockchain is the technology in which a unique event occurs at a certain time that the event can have a transaction of ID creation or any document. It is important to understand that only a hash is added on the blockchain without giving any transaction information. Without the centralized entity, blockchain is a system that stores information in distributed networks of personal computers. A secure computer system includes all the computers in the network having the same database information. The health-care system lists all the medical reports with secure hash authentication and data protection. Dealing, executed between doctors and patients, is a time stamp and immutable that means once you add any transaction information to the blockchain, you cannot go back and change it or delete the people from the network. Medical report/s listing is secure with an algorithm that provides them with a unique hash. This health-care system helps one to save time, money and facilitates the doctor to treat the patient after getting the approval from the patient to access the medical records. It also

¹Acharya Motibhai Patel Institute of Computer Studies, Ganpat University, Mehsana, India

helps other organizations, that is, health-care industry, insurance agency, the pharmaceutical industry, and research organizations to analyze and improve the services.

Multinational companies are contributing in the following different ways to expand the economy:

- Improve the quality of the medicine.
- Invent new drug to deal with the newly detected disease.
- Increase the value care of citizens in the developing country.
- Help one to expand the economic opportunities.
- Big organizations help one to expand the possibilities in the field of new employment, training of the person and also improve the infrastructure across the nation.
- Employ thousands of developing countries.

A team of researchers mention in report [1] on how pharmaceutical industry participates in expanding economic opportunities in developing countries.

15.1.1 The laws of privacy

Security research in the European Union has mentioned in the example how present discourse on privacy can be affected due to the joining of ethical and legal privacy [2].

Privacy is an important and critical factor of any citizen across the nation. Different nations design different laws related to privacy whenever you are gathering personal information of a citizen. This private information may be the name of a person, residential address, birthplace, business or home telephone number, mobile number, social security number, physical description, etc. In the world, different nations have designed their own acts related to privacy and they are also endlessly improving the laws of the country. Some of them are as follows:

- As per federal requirements, the United States composed acts, namely, “The California Online Privacy Protection Act (CalOPPA)”. In 2004, CalOPPA operated to protect the privacy. Later, due to updates in new technology and the emerging demand of online users, it was updated in 2013.
- To handle commercial activity, personal information is very critical and sensitive. In Canada, Department of the Privacy Commissioner of Canada implemented the act “The Personal Information Protection and Electronic Documents Act (PIPEDA).”
- Under the Australian government, the Office of the Australian Information Commissioner applied the secrecy law “The Privacy Act 1988” that regulates how to handle private data, such as an individual’s name, signature, address, business or home phone number, birthdate, birthplace, health-care reports, statement of bank account, and views about a character. Australian Privacy Principles are made of 13 Australian privacy policies, the privacy of which is applicable to different Australian sectors. These sectors cover both government and private organizations.

- India has also submitted a 176-page report and proposed a policy of privacy to protect personal data in 2018. The proposed “Data Protection Bill, 2018” essentially makes individual consent central to data sharing.
- Due to technology advancement, China is also planning to organize the cross-border transmitting of private information of the person and also proposed the “Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data.”
- On October 24, 1995, the European Parliament and the Council processed the Directive 95/46/EC to protect an individual against the use of private data of the person and easy transfer of the information.

15.2 History of concerning issues

15.2.1 Traditional health-care system

In the traditional health-care system, there is no availability of a central database to store patient data for future use. Even medical health-care data is used only once and later discarded. Here, we have tried to explain the earlier system that is very similar, as explained through Figure 15.1. There are two towns, namely, north and south, respectively, and both have separate health-care system. For basic treatment, people can take treatment from individual doctors, named A and B, but there are

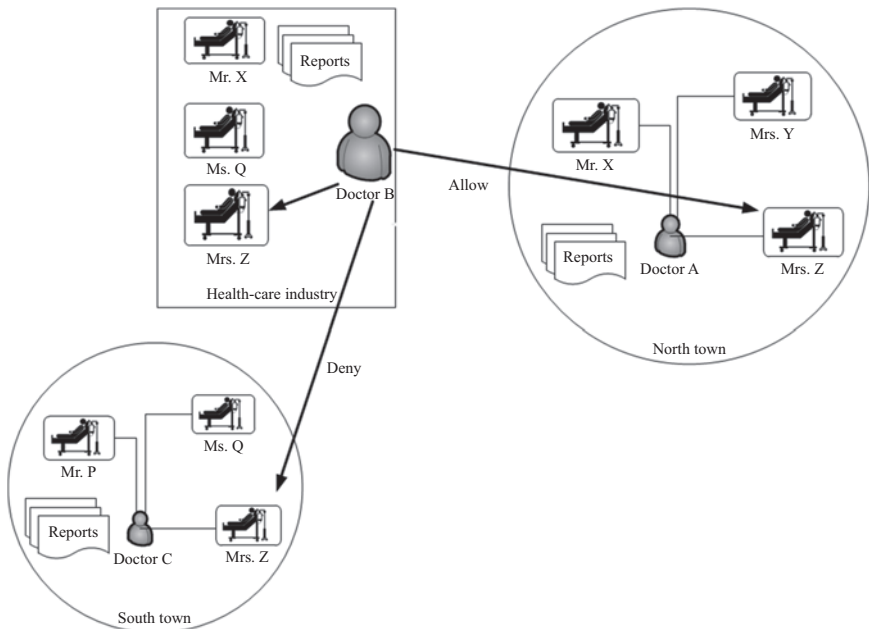


Figure 15.1 Traditional health-care system

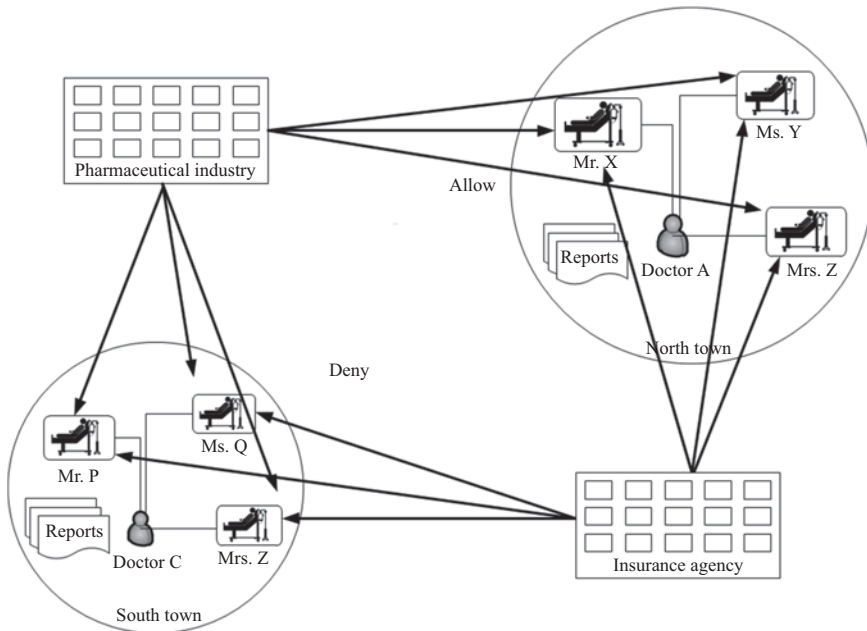


Figure 15.2 Traditional pharmaceutical industry and insurance agency

certain emergency cases in which Mrs. Z has to be admitted to a health-care hospital. Here, Doctor B is unable to find the history of Mrs. Z. This will take more time to get the latest report of the patient. New report generates task and also increases the cost of treatment and a few critical cases, such as permanent organ loss or death, which can be possible.

Pharmaceutical organizations/insurance agencies are also struggling with the earlier system—see Figure 15.2. Due to unavailability of the patient’s data, it is difficult to improve the existing drug and develop a new drug. Insurance agencies also require patient’s data to reduce the process of insurance claim. In some cases, health organizations or individuals are ready to share the patient’s data, although this circumstance does not happen everywhere. Some organizations deny access of patient’s data.

15.2.2 History of health care

World Health Organization, WHO, plays an important role to observe the health of persons across the world. Since 2005, every year WHO has been announcing the report “World Health Statistics Series” to know the trend of the world’s health. Majority of developed nations keep the primary goal of their government to serve citizens in an easy way with minimum cost. WHO focuses on different health-care goals, such as procreative, maternal, infant and baby health, transmissible infections,

noncommunicable diseases, and mental strength, Universal Health Coverage—UHC, environmental risks, fitness risks, and sudden occurrence of disease [3].

WHO report

The monitoring of effective service coverage report focuses on the following three different challenges:

- Effective service coverage
- Effective planning of service area
- Observing the equity in access to standard health service

15.2.3 History of data protection

In the last decade, the Internet of Things (IOT) not only introduced huge opportunities and advantages in the field of health care but also proposed upcoming difficulties. A team of researchers identified the security issues and also tried to explain the “How to deal?” [4].

In 2017, Department of FBI—Internet Crime Complaint Center (IC3) received 4 million consumer Internet crime complaints. These complaints are registered against criminals, overseas adversaries, and terrorists. IC3 admitted a total of 301,580 grievances with reported damages exceeding \$1.4 billion. These crimes were divided into different categories such as nonpayment/nondelivery, personal data breach, and phishing. IC3 also asked the citizens to preserve the nation against cyber warnings [5].

15.2.4 History of blockchain technology

In 2008, Satoshi Nakamoto made blockchain (a block connected to the previous block except for the root block) to assist as the free trade ledger of the cryptocurrency bitcoin [6].

In the last decade, the Bitcoin Association has received great attention toward the blockchain. In a decentralized fashion, blockchain helps one to create changeless ledger that permits the transaction. There are different popular applications derived from blockchain concept, such as privilege regularity, business assistance, well-known technology IOT [7].

William J. Gordon and Christian Catalini have also shown the possibility of how blockchain can help in areas, such as access rights of digital private information, collecting private information, information sharing, profile of the patient, and information immutability. Moreover, they also discussed the most critical barrier of sharing patient’s data to the blockchain [8].

The IOTA Foundation developed the IOTA protocol that serves as distributed ledger technology. Due to the key quality of lightweight and malleable, the IOTA protocol is used to preserve privacy in devices of the IOT. It is an open-source distributed ledger. The objective behind this protocol is to develop such a system that not only produces open services but also preserves the privacy between devices. The IOTA protocol provides various features, such as sharing and saving of data, and access to the secure process [9].

15.2.5 Transaction of blockchain life cycle

- Step 1: Call for transaction.
- Step 2: A block that represents the creation of transaction.
- Step 3: The block is broadcasted in distributed networks to every node in the network for validation.
- Step 4: Each node receives the request to validate the transaction.
- Step 5: Each node receives a reward for the proof of work.
- Step 6: The block is appended to existing blockchain.
- Step 7: The transaction is executed.

Example: *Blockchain class block in Java*

A blockchain consists of different blocks. These blocks are connected to each other.

```
// Import Date Package
import java.util.Date;
public class Block {
    // Defining Variable Private/Protected/Public
    public String hashBlock;
    public String previousHash;
    private String dataBlock;
    private long timeStamp;
    // Basic Class Structure of Block
    public Block(String dataBlock, String previousHash) {
        // Block Data can be extended as per the user needs
        // Data of Block which need to be encrypted
        this.dataBlock = dataBlock;
        // Reference of Previous Block
        this.previousHash = previousHash;
        // Current Date and Time
        this.timeStamp = new Date().getTime();
    }
}
```

Generate digital signature

String hash is used to store the digital signature.

```
import java.security.MessageDigest;
public class StringUtil {
    //Applies Sha256 to a string and returns the result.
    public static String applySha256(String input) {
        try {
            MessageDigest digest =
                MessageDigest.getInstance("SHA-256");
            //Applies sha256 to our input,
            byte[] hash = digest.digest(input.getBytes("UTF-8"));
            StringBuffer hexString = new StringBuffer();
            // This will contain hash as hexadecimal
            for (int i = 0; i < hash.length; i++) {
                String hex = Integer.toHexString(0xff & hash[i]);
```

```

        if(hex.length() == 1)
            hexString.append('0');
        hexString.append(hex);
    }
    return hexString.toString();
}
    catch(Exception e) {
        throw new RuntimeException(e) ;
    }
}
}

```

Hash calculation

```

public String calculateHash() {
    String calculatedhash = StringUtil.applySha256(
        previousHash +
        Long.toString(timestamp) + data
    );
    return calculatedhash;
}

```

Constructor of block

Constructor has the same name as the class itself. Constructors do not have return type. A constructor is automatically called when an object is created.

```

public Block(String data,String previousHash ) {
    this.data = data;
    this.previousHash = previousHash;
    this.timestamp = new Date().getTime();
    this.hash = calculateHash();
    //Making sure we do this after we set the other values.
}

```

Examples of blockchain

```

public class HealthChain {
    public static void main(String[] args) {
        // Create Root Block
        Block rootBlock = new Block("Roo Block", "0") ;
        // Hash of 1st Root Block
        System.out.println("Hash" + rootBlock.hash) ;
        // Create 1st Block after root Block
        Block firstBlock = new Block("1st Block", rootBlock.
            hash) ;
        System.out.println("Hash" + firstBlock.hash) ;
        // Create 2nd Block after root Block
        Block secondBlock = new Block("Hey im the third block",
            secondBlock.hash) ;
        System.out.println("Hash for block 3 :" + thirdBlock.
            hash) ;
    }
}

```

15.2.6 *In what way blockchain technology could transform our lives*

The blockchain has given the proof of work with the creation of digital currency known as bitcoin. Bitcoin value has been steadily growing since 2015 [10]. Following are the different areas where humans can use the technology and have the ability to transform lives:

- With different goals and features, creation of other currency is also possible.
- Due to its unique feature, it can also be used in nonfinancial transaction, that is, election vote system.
- Blockchain also helps in solving the significant obstacles of privacy in the film industry.
- Public services, such as health care and welfare payments.
- Smart contracts help in digitalization of documents and proof of ownership for transfer.
- Property market can store property document in digital format.
- It enables to trade digitally in the stock exchange.

15.3 System design

Following are the core components of health-care blockchain technology. These core components, directly or indirectly, participate in the system for a smooth execution of block chain.

15.3.1 *Security principle*

There are three main security elements that need to be proposed by any security purpose: (1) confidentiality, (2) integrity, (3) availability. It is also known as CIA (Figure 15.3).

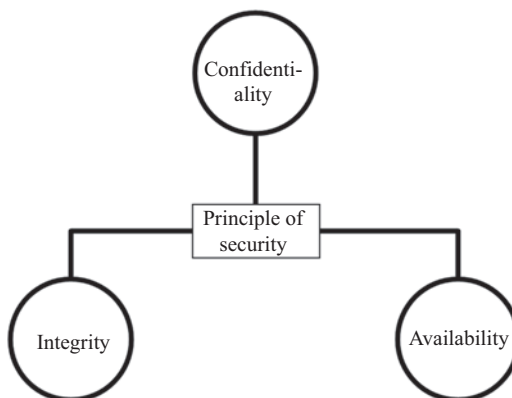


Figure 15.3 *Basic principle of security*

Confidentiality makes sure that only the authorized user is able to read the transaction. Integrity makes sure that the sent communication is received at the destination without any modification, and availability means that each service or data is available to the user when it is demanded.

- *Confidentiality* decides the access level of the patient's data. It means who have access to medical records. Medical data can be classified by a degree of confidentiality. The access level of the patient's data is restricted to prevent attackers from gaining access to critical data. Encryption/Physically safeguarding also helps one to maintain the confidentiality of data. The process of cryptography helps one to convert patient's data into an encoded format so that only the approved health-care subject can read his/her private medical reports. If anyone gets this data, it is difficult to read due to data in an encrypted format. Social engineering is also used to break security. Security awareness program can help one to prevent these types of attack.

Possible attack: Monitoring attacks.

The consequence of attack: Attackers are continually monitoring traffic to know the confidential information of users, that is, username, password, secret question, one-time password, and email activation link.

- *Integrity* is used where medical records are accurate and readable. Collected data stored without integrity is useless. Proper guidelines and training help one to ensure the fact that collected data is from trusted patients.

Possible attack: Message alteration attacks.

The consequence of attack: Attackers try to alter the original message from the source to the destination. Malicious viruses are attached with original software or messages.

- *Availability* is related to access to the data and when it is demanded. In emergency cases of health care, the doctor needs to immediately check the history of the patients.

Possible attack: Denial of service attack, jamming, malware, and spamming.

The consequence of attack: Network facilities are not accessible for network users. Attackers create network jam situation by sending continual requests on the server. There are certain limitations of network resources. Due to heavy traffic on the server side, the server crashes or becomes unable to respond to the users.

15.3.2 Distributed network

The network system is divided into two broad categories: centralized and distributed as shown in Figure 15.4.

Centralized system

In a centralized network system, all users are connected to a central network. A central network works as a single agent for all communication. A single database is located at one place. The following are the advantages and disadvantages of a centralized network.

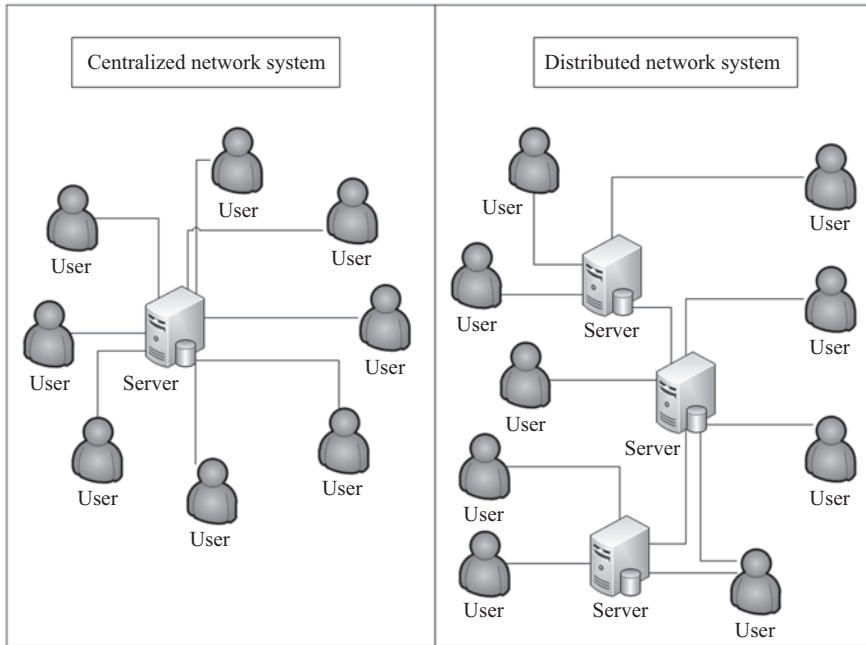


Figure 15.4 Centralized vs distributed network

Advantages

- Single database for all records.
- Easy to manage, update, and back up all the data.

Disadvantages

- Network services are unavailable for all if network system fails.
- Once data is lost, it is difficult to recover the data.
- A slower performance of network as a considerable number of users are accessing a single network system.

Distributed system

In the opposite of centralized network system, all the users are connected to a different network. There are multiple networks to connect the users. It also keeps multiple copies of the database on different servers. The following are the advantages and disadvantages of the centralized network system.

Advantages

- Improves the performance since records are accessible from the nearest destination.
- Network services are available if any network system fails within the network.
- Easy backup due to multiple copies of the database.
- Openness and scalability.
- Sharing of resources.

Disadvantages

- Much time is required for synchronization.

15.3.3 Patients

Patients are a primary key entity of this system, who require health-care assistance for various diseases. Whenever patients are admitted in the hospital for medical treatment, the doctor has to perform a number of reports for diagnosis. In a normal scenario, these reports are used for a limited number of times and later discarded. There is no secure storage system so that it can be reused in the future. Primary, a minor treatment of health care can be treated through individual doctors but in severe cases, the patient has to reach the medical organization or the expert doctor. To handle patient's case carefully, the doctor needs to perform a number of medical tests and compare these tests with the earlier case. This activity is also known as the history of the patient. Blockchain helps one to store patient's data in an encrypted format. This data can be used again if the patient gives his/her concern to doctors, health-care organization, pharma industry, insurance agency, etc. The following are the key features of storing patient's data in system as shown in Figure 15.5.

- At the time of the patient's care, the doctor can get correct and the latest updated records of the patient.
- Efficient care is possible due to easy access of records from the cloud.

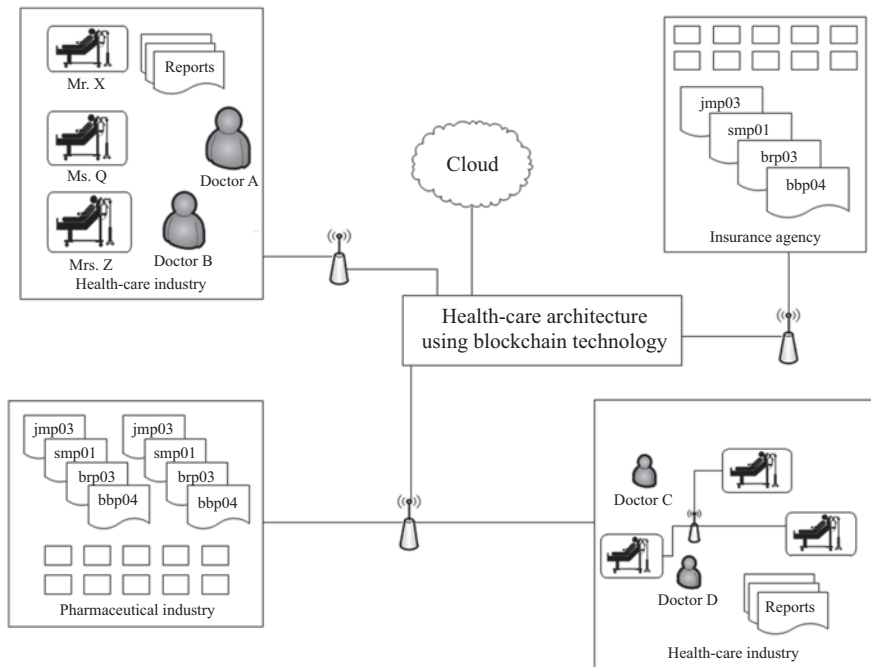


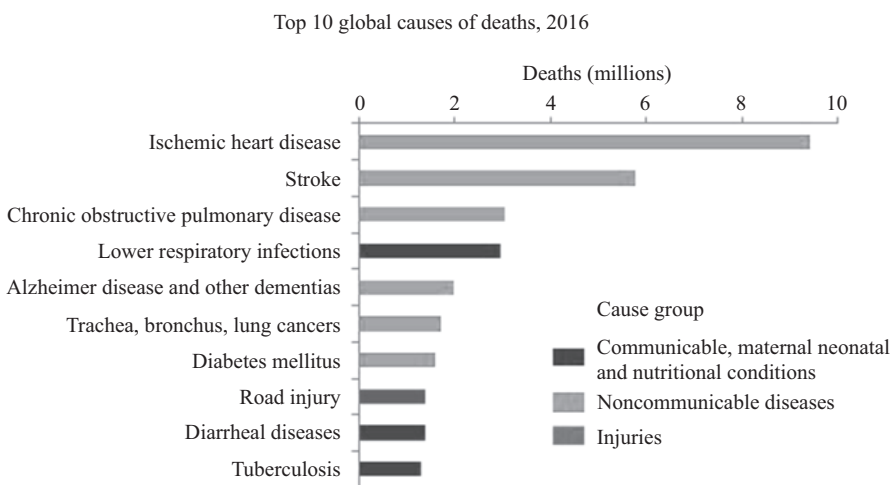
Figure 15.5 Proposed health-care architecture using blockchain technology

- Patient can securely share the medical reports with other individuals/ organizations.
- To effectively diagnose sufferers, medical history plays a significant role in reducing medical mistakes and providing instant care to patients.
- Provides an additional layer of secrecy and safety to medical records.
- Reducing costs repetition of reports.

15.3.4 *Doctors*

A doctor, the most respected name very next to god, has a prime objective to treat patients. He/She has to deal with different diseases while treating the patients; a small amount of time is very valuable since it is a matter of life and death. A small delay in the treatment may create a loss of organ/s, and in severe cases, death is also a possible cause. WHO published a report in 2016 and as per this report, they have found some significant facts in the health-care sector as shown in Figure 15.6.

- The number of deaths worldwide is 56.4 million in 2015.
- There are many incidences of diseases in health care, which are somewhat preventable.
- The reason behind the death of 56.4% of cases out of 68% is diseases that progressed gradually.
- There are unpreventable factors, such as personal lives, use of defensive care, and standard of health care.



Source: Global health estimates 2016: Deaths by Cause, Age, Sex, by Country and by Region, 2000–16. Geneva, World Health Organization; 2018.

Figure 15.6 Global causes of deaths in 2016

15.3.5 Internet service provider

Now, the world is connected through the Internet. It plays a major role in the revolution and due to this change, the distance between people has become very less. Major Internet service providers are continuously trying to improve the services throughout the nation, and they are satisfactorily achieving their goals by providing speed and availability throughout the nation.

15.3.6 Health-care industry

In the health-care sector, medical organizations play a key role in treating the patients for various diseases. The prime objective of medical organizations is to provide instant, low cost, and error-free medical care. It is difficult to provide health-care treatment for all the diseases by only one hospital. Different hospitals have different specialties in treating diseases. Sometimes, a clinic needs to share the patient's report to other organizations to avoid delays in critical conditions and because of the extra cost of report, due to privacy and security, they refuse to share it.

15.3.7 Cloud

Cloud services are the most essential tools for storing data online digitally. Amazon Web Services, Microsoft Azure, Google Cloud Platform, VMware, IBM Cloud are popular service providers that have contributed to the development of cloud awareness. The traditional way to store an organization's data is the in-house server. People from various organizations maintain their own servers to store the data. Security is the significant issue of the earlier system. The primary advantages of storing files on the cloud are speed, low cost, access from anywhere in the world. The following are the top advantages for storing data:

- *Universal accessibility:* Cloud provides accessibility of data from different locations throughout the nation. Due to continuous advancement, users are now able to access cloud data through mobile, laptop, computer, etc. via the Internet.
- *Recovery in disaster:* Natural emergencies happen due to alteration of the cycle of nature, such as flood and earthquake. It is extremely suggested that a backup option should be available to protect important data. Cloud storage of data for multiple reasons is essential to protect this data so that other copies of data can be used if the original is lost.
- *Security with encrypted algorithm:* Top companies are providing the cloud facility, such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, VMware, IBM Cloud. Researchers are contributing toward improving security through deep research on security and exploring the issues of secure storage space, unauthorized access control, transaction alteration, monitoring, etc. [11].
- *Price reduction:* Today, a large number of nations realize the power of information technology and how technology gradually improves the lifestyle of

people. It is difficult to develop the resources across different regions of the nation. Sometimes it is difficult to use 100% resources. Cloud helps one to reduce the cost of the resource due to the feature of universal access [12].

- *Easy sharing*: Nowadays, information technology helps easily to share the text, graphic, music, video, image, etc. with other users. There are key benefits of document sharing, such as cost reduction, storage space, easy accessible, collaboration work, and many more.
- *Expandable services*: Across the world, the population is growing. To fulfill the huge requirement of resource, demand is also rising. It is easy to expand the services with the help of cloud as resources are managed in a centralized manner.
- *Automated trigger*: Automation helps one to execute tasks automatically when an event occurs with the help of a trigger.
- *Easy synchronization*: Data synchronization refers to the process of establishing continual bridges between source and destination data and vice versa. This fundamental process is widely used in applications, such as Google drive and mobile device. In the absence of Internet connectivity, data is stored off-line and on getting Internet connectivity, data is synchronized between origin and target.

15.3.8 *Insurance agency*

In India, to fulfill the high growing demand of insurance industry, more and more companies are now emerging. A motto of insurance is to protect the family from any uncertainty in life. The life insurance sector in India is the largest in the world. There are around 360 million policies and every year they are increasing regularly. The growth rate will be around 12%–15% in the next expected year. The health-care sector helps in serving people in efficient ways, such as safety and security that promotes economic growth, the spread of services in rural areas [13].

There are several popular names of universal health care, such as UHC, universal coverage, universal care, or socialized health care. The organization helps in serving citizens of the particular nation through the activity of financial assistance and health-care services. To fulfill the specific goal of health care, the organization provides different packages to improve the health of citizens [14].

15.3.9 *Pharmaceutical industry*

The pharmaceutical industry is performing life cycle of drug development on a regular basis to increase the quality. This cycle includes tasks, such as discovery, development, and production. Researchers require the database of patients to find new knowledge so that they can contribute to society. MIT Lab for Computational Physiology serves the database of around 40,000 patients. The primary objective of this database is to supply medical patient's data for research. The researcher may get free and paid database of medical records to find new facts to serve the society.

Preserving public health is a leadership challenge of any government. The Food and Drug Administration (FDA) is verifying the protection, effectiveness, and

safety of humans in the USA. FDA also mentioned the steps of the drug development process:

- Research helps in discovery and development of new drug.
- Preclinical research helps in answering the basic health-care questions.
- In clinical research, drugs are tested on humans to check basic safety.
- FDA determines the result (accept or reject) related to new drug based on the investigation of all the relevant data.
- Drug authority also monitors the drug when it is launched for public use.

15.4 The blockchain-based health-care industry

Whenever a patient is admitted to the hospital for treatment, the doctor has to perform a number of tests to know the current condition of the patient. Earlier reports are discarded due to lack of a secure platform. Blockchain technology helps in storing this data for future use if needed. The primary advantage of blockchain technology is security. Blockchain stores just the transaction ID in a header and the remaining transaction information is stored in the body of the block. Table 15.1 shows the different parameters of the block header of blockchain.

Following are the different parameters for designing block chain header.

#: It stores unique identification number of block.

Patient ID: Unique identification of the patient. It may be e-mail, mobile number, or unique code provided by the nation.

Request by: A person or organization may need to require access to the patient's health-care record. This file can differ based on different situations:

- An individual doctor may demand the patient's reports if he/she requires to know the history of the patient. Based on these reports, the doctor can compare the current report with the earlier report. To improve the health of the patient, the doctor may change the current medicine dose or continue the previous treatment to improve the health condition.
- The insurance company has to deal with various situations whenever a claim is registered by the patient to process the insurance amount. In some cases, due to lack of proper platform, frauds can occur. Before issuing any medical policy, an insurance company can check the history of the patient's report. It will not

Table 15.1 Design of block header

#	Patient ID	Request by	Access type	Hash	Device ID	Action
01	jmp03	Doctor01	Read	Key	MAC01	Allow
02	smp01	Insurance01	Write	Key	MAC03	Allow
03	brp03	Health01	Execute	Key	MAC02	Allow
04	bbp04	Pharma02	Read	Key	MAC01	Deny

only help the organization to prevent the fraud but also increase the speed of the process linked to the insurance policy.

- In normal cases, the patient can take treatment from the doctor's clinic and resolve the disease problem but in a severe case, the patient has to consult a hospital where he/she can take the treatment from the health-care team. Similar to individual doctors, the hospital also needs to know the history before treating the patient.
- Humans are continuously finding new facts through the process of research. Researchers are being able to predict and analyze the effect of the drug. With prior permission from patients, they are able to get the records. This record helps in-depth study.

Access type: This field is used to decide the access type of the patient's record. This access type is broadly divided into three different operations, that is, read, write, and execute. In addition, different access types can also be added if a user wants to expand this system as per requirement. In fact, in different situations, different access permissions are required.

- *Read:* This permission is used for reading the data of patients from his/her medical record profile.
- *Write:* The patient has to pass a number of medical tests while in diagnosis for medical treatment. These reports require writing the access permission for storing data in the database for further use.
- *Execute:* In some cases, read and write operations are both required for smooth execution.

To preserve the security and privacy of patient's health-care records, blockchain does not add medical report information in the block header. Important information is stored into the body of blockchain with the following parameters. Health-care blockchain technology helps one to decide the data access of the authority. Prior to access to patient's data, the authority needs to take permission of the concerned patient. These authorities can be an individual doctor, health-care organization (hospital), insurance agency, pharmaceutical industry, etc. Table 15.2 shows the different parameters of blockchain transaction.

Block transaction ID: This field is used to store the blockchain transaction unique identification number. This ID also maps the ID of the blockchain header. In the first transaction of the block, it stores the original value that is also called the root value.

Table 15.2 Design of transaction

Block transaction ID	Previous block ID	Time stamp	Device ID	Digital signature
01	Root	04-08-2018, 2.07 AM	Unique ID	Signature of jmp03
02	01	12-08-2018, 2.07 PM	Unique ID	Signature of smp01
03	02	28-09-2018, 2.07 AM	Unique ID	Signature of bbp04

Previous block ID: In blockchain, the block is arranged in linear fashion. It means that all blocks are connected to each other in a sequential manner. Unique identification ID of the preceding block is required to join the current block to the previous one. Please take note that there is no previous block ID of the first block. The first block has stored the value of the root, that is, a child without any parent.

Time stamp: It is important to store patients' data with a time stamp. Time stamp includes date and time so that the doctor can know the complete history of patients' record.

Device ID: Digital record is accessed through electronic devices, that is, mobile, computer, laptop, etc. The manufacturing company provides the unique hardware ID that helps one to identify these devices. It helps one to know the device used to access the data of the patient's medical record.

Secure electronic mark: The digital signature is the guarantee of a secure message transmission. When a transaction is submitted on the network, the digital signature helps one to secure the transaction through the private and public key. There are different categories for different uses. These categories include the visible signature, invisible signature, approved signature, certified signature, etc. for data access of the authority. Prior to access to patient's data, the authority needs to take permission of the concerned patient. These authorities can be an individual doctor, health-care organization (hospital), insurance agency, pharmaceutical industry, etc.

Key generation: An algorithm such as RSA is used to generate the private and public key. These keys are used in either digital signature creation or verification of digital signature as shown in Figure 15.7.

The process of digital signature creation using private key is as follows:

The sender submits input files or messages for the creation of a digital signature. These documents need to compute cryptographic hash with the help of algorithm, such as SHA-256, SHA-384, SHA-512, or Whirlpool. The private key is used to create an encrypted hash. Encryption is the process of converting plain text to ciphertext. First, this digital signature is attached to the documents and later, it is sent to the receiver for verification of the signature.

The process of digital signature verification using public key is as follows:

As shown in Figure 15.8, the receiver computes the cryptographic hash of the received file or message by using the same hashing algorithm. The receiver decodes the digital signature with the help of a public key. If the decrypted hash is

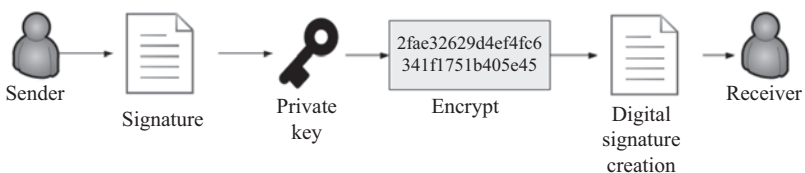


Figure 15.7 Digital signature creation using private key



Figure 15.8 Digital signature verification using public key



Figure 15.9 Graphical representation of secure health-care blockchain

exactly the same as the computed hash of the received file, it means that the digital signature is verified and the data was not tampered with during transit.

Life cycle of health-care system based on blockchain technology:

- Health-care organizations provide treatment to patients.
- During treatment, all of the health-care data of patients is measured and stored with the help of health-care blockchain technology.
- Reports are stored as per the design of the block (see Figures 15.9 and 15.10).
- Each transaction is stored on the blockchain. Only the block header is accessible while block transaction information is not accessible.
- Health-care organizations and other authorities can access this data with prior information from patients.
- On other hand, to preserve the privacy of patients, he/she can take the decision regarding the sharing of the data himself/herself.

15.4.1 Benefits of health-care blockchain

Advantages of blockchain technology in health-care industry are as follows:

- *Secures the health of citizens:* In major countries, health of the citizen is a primary objective for economic growth. The regulatory body of the nation may develop and maintain the system so that health of citizens can be monitored. This monitoring will help in a number of ways. In earlier stages, a disease can be identified so that it can be prevented from spreading to others. Economic growth also depends on the health of the citizen.
- *Database for research:* Research is a process of finding new knowledge. There are various categories of people who are performing research to make life

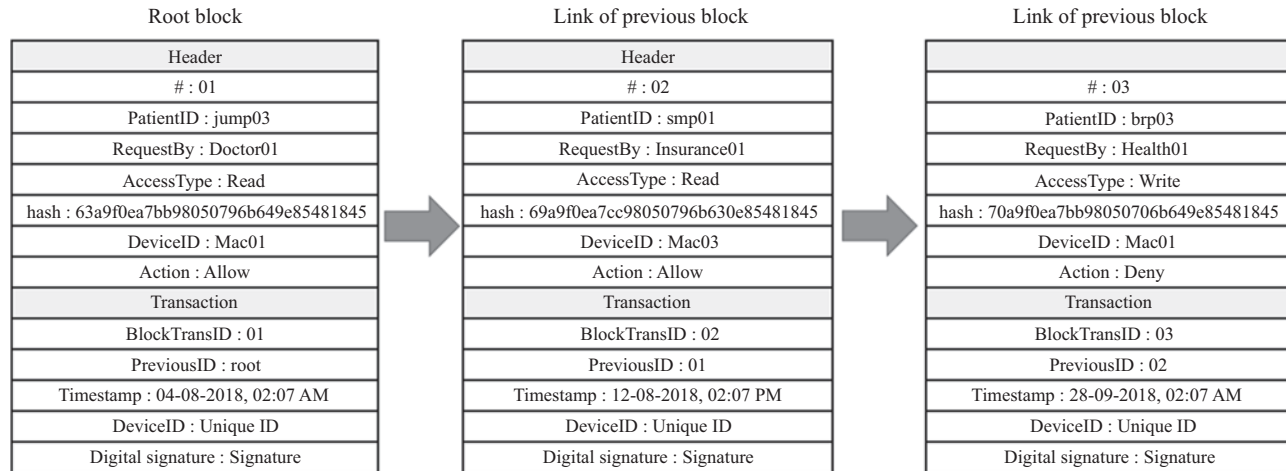


Figure 15.10 Design of health-care structure of block

better. These categories include student groups, group researchers, private or government bodies, etc.

- *Improves the drug:* Due to the change in environment, every day, new diseases are detected. The pharmaceutical organization fulfills the requirement of the drug. It may be possible that there are multiple drugs for the same disease. This happens because more than one company might be developing the same drug. Medical firms are continually trying to improve the quality of the drug so that they can compete with the competitor.
- *Invents/Develops new drugs:* Since the last decade, the world has been witnessing new diseases. The research team has to develop drugs to fight these diseases. Without a patient's health-care monitoring data, it is difficult to develop a new drug. These data will help in studying the effect of the disease.
- *Data security:* Blockchain concept is popular for security since it stores unique blocks in the immutable chain. Bitcoin is a cryptocurrency designed around the concept of the blockchain. It is a decentralized digital currency without a central bank.
- *Data privacy:* Privacy of the patient's data should be maintained. It is difficult to maintain privacy in the absence of a secure platform. In health care, blockchain is a concept that will fulfill this gap. Citizens of the nation can decide the access of their own medical data.
- *Minimizes the cost:* The health-care blockchain technology helps one to minimize the cost across the country. There are cases in which some cases need to be performed due to interoperability of health-care records.
- *Economic growth:* With the help of the system, health-care sector improves the quality of medicine and quality care for citizens of the country. It also expands opportunities through job creation, shaping policy, research, etc.

15.4.2 *Challenges of health-care blockchain*

Blockchain has the ability to transform the health sector. The technology helps in designing a patient-oriented system to preserve the privacy, security, interoperability of electronic health-care records. Opposite to the opportunities, it also comes with challenges [15]. Following are the common challenges to operate blockchain in health care:

- *Exchange and interoperability of electronic health-care records:* The exchange of electronic medical records is a crucial thing in the health-care system. Blockchain-based health-care information systems can solve the problem of privacy, security, interoperability, and integrity. However, due to the existing privacy act of various nations, the interoperability task looks much more challenging.
- *Unwillingness to publish data:* There are several incidences that have happened in which medical organizations have not been willing to share the expense of treatment with other hospitals or the insurance industry. The primary reason for this is patient-wise variation in treatment cost. Execution of advanced technologies is a difficult task.

- *Health care is divided:* In the current scenario, the medical organization and insurance industry are in the distributed format, which means that there is no synchronization between these two sectors. Hence, accepting blockchain technology in health care is doubtful. Execution will also be difficult if either of the parties will access the changes.
- *Significant social transformation:* In short, the duration to shift from manual to electronic record is a difficult task. Alteration of patients' reactions is also a challenging task. Resistance from the employees is also a possible cause.
- *Lack of proven use cases:* It is difficult to adopt health-care technology until health-care market leaders and complete training is procured and provided, respectively. Due to the lack of proven use cases, nobody is willing to come together and work on a solution.
- *Cybersecurity in electronic health care:* New cybersecurity vulnerabilities are introduced because of interconnections in the health-care sector. Lynne Coventry and Dawn Branley review and explore the following critical areas [16]:
 - Health care is a vulnerable entity.
 - Health care is a targeted entity.
 - Various types of threats and consequences are being experienced currently.
 - The role of legislation and standards.
 - Health-care sector has barriers that prevent moving forward.

15.5 Future trends

Estonia has already taken the first step toward blockchain technology in both government and private sectors [17]. Health-care applications are being developed and spread across the country with the help of governing authorities and private startup companies, such as Guardtime, to use secure public and private ledgers. With regard to blockchain technology in health care, Estonia demonstrated how innovation is a process through GovTech. IOTs enable humans to get a greater level of automation by developing a system using sensors, interconnected devices, and the Internet. In ICU, patient monitoring is a difficult and the most important activity where a small delay in decision related to patients' treatment may cause permanent disability or even death. Most ICU devices are equipped with various sensors to measure health parameters but to monitor it all the time is still a challenging task. Proposing an IOT-based system can help one to easily communicate and identify emergency and initiation of calls with health-care staff, which helps one to start proactive and fast treatment. This health-care system reduces the possibility of human errors and delays in health-care treatment and helps the doctor in sparing more time for a decision with accurate observations [18].

There is a dearth of skilled medical experts in developing countries such as India, as various health challenges and crises due to a high growth of population are faced by patients who are required to be treated in hospitals. In the proposed research model, a system needs to be developed, which will connect doctors to

hospitals that need their expertise for the treatment of patients. The system allows capturing patient's health-care data, stored in the database, and transmitted via cloud through various sensors attached to patient bodies. Based on patient's data, basic, voluntary doctors can suggest appropriate treatment and medicine dose based on health-care data and treatment requirement. It may save the life of the patient and further, this platform may be helpful for sharing opinions by analyzing patients' changing health-care data [19].

15.6 Conclusion

Nowadays, the world is facing lots of problems in health care. New diseases have also been introduced since the last decade. Possibility of blockchain for health care highly depends on the people who can readily accept this new technology in health care. The government has to spare an amount to develop the necessary infrastructure and train the people in minimizing the cost of health services across the country. However, there are still many challenges of blockchain technology such as scalability.

Health-care technology using blockchain plays an important role in economic development and health of citizens, but it also faces problems such as security vulnerability threats due to interconnected, easily accessible access points, outdated systems, and a lack of emphasis upon cybersecurity. There are vast amounts of valuable, sensitive data, which is sometimes used for financial gain. Medical identity is more worthy than other identity credentials. Other crimes may be driven by political gain, even cyber warfare. However, if critical health systems are attacked, human lives will be at risk [16].

References

- [1] A. Mahmud and M. Parkhurst, "Expanding economic opportunity: The role of pharmaceutical companies. Corporate social responsibility initiative report no. 21," 2007.
- [2] Gloria González Fuster, Serge Gutwirth, "Ethics, law and privacy: Disentangling law from ethics in privacy discourse," *IEEE International Symposium on Ethics in Science, Technology and Engineering*, 2014.
- [3] D. T. A. Ghebreyesus, "World health statistics," 2018.
- [4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. C. Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Network*, vol. 76, pp. 146–164, 2015.
- [5] S. S. Smith, "Internet crime report," 2017.
- [6] Wikipedia, "Blockchain," 2018. [Online; accessed 05 December 2018].
- [7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," *IEEE 6th International Congress on Big Data*, 2017.
- [8] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 224–230, 2018.

- [9] J. Brogan, I. Baskaran, and N. Ramachandran, "Authenticating health activity data using distributed ledger technologies," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 257–266, 2018.
- [10] P. Boucher, S. Nascimento, and M. Kritikos, "How blockchain technology could change our lives," 2017.
- [11] R. Wang, "Research on data security technology based on cloud storage," *13th Global Congress on Manufacturing and Management, GCMM 2016*, vol. 174, pp. 1340–1355, 2017.
- [12] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, 2015.
- [13] P. J. Kumari, "Role of insurance in economic development of India," *Computer Network*, vol. 2, no. 12, pp. 1636–1637, 2016.
- [14] Wikipedia, "Universal health care," 2018. [Online; accessed 21 October 2018].
- [15] K. Rabah, "Challenges and opportunities for blockchain powered healthcare systems: A review," *Mara Research Journal of Medicine and Health Sciences*, vol. 1, no. 1, pp. 45–52, 2017.
- [16] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.
- [17] T. F. Heston, "A case study in blockchain health care innovation," *International Journal of Current Research*, vol. 9, no. 11, pp. 60587–60588, 2017.
- [18] P. Bharat, P. Satyen, and P. Jignesh, "An intelligent real time IOT based system (IRTBS) for monitoring ICU patient," *Information and Communication Technology for Intelligent Systems*, vol. 2, pp. 390–396, 2017.
- [19] P. B. P. S. Jignesh, "Effective healthcare services by IOT-based model of voluntary doctors," *Data Science and Big Data Analytics*, Singapore: Springer, pp. 109–116, 2018.

This page intentionally left blank

Chapter 16

Blockchain-powered healthcare insurance system

Hardik Gajera¹, Manik Lal Das¹, and Viral Shah¹

Security and privacy concerns of health records are challenging issues in modern healthcare systems. Typically, in a healthcare system, doctor requires to confirm the legitimacy of patient's health records prescribed by pathological laboratories; insurance company needs to check the validity of medical/diagnosis reports submitted for the insurance claim; and patient requires to ensure his/her health records privacy protection while consulting with different parties (e.g., doctor, nurses, and laboratory staff) involved in healthcare system. Furthermore, health records should not be perceivable to unauthorized parties with malicious intentions on patient's health. Therefore, confidentiality, integrity, and privacy of health records should be preserved while transmitting health records over communication channel and/or while storing data on a third-party server. In recent times, blockchain technology shows potential for publicly verifiable and immutable transactions while managing records in a decentralized system. In this chapter, we discuss about the applicability of blockchain technology for protecting health records with respect to tamper-proofing, accountability, ownership, and data privacy. We present a healthcare system powered by protocols using blockchain technology that ensures accountability and transparency of services availed by different entities involved in healthcare system. The proposed protocols address the issue of ill-formed medical report for availing/denial of health insurance, which is a practical problem that needs effective solution from both claimant and service provider. The proposed system addresses this important issue, where the patient can avail deserving service from the insurance company and the insurance company can confirm the legitimacy of the medical report.

16.1 Introduction

Security and privacy concerns of health records are challenging issues in healthcare systems. Doctors need to confirm the legitimacy of patient's health records received from pathological laboratories; insurance companies need to check the

¹Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, India

validity of medical/diagnosis reports submitted for the insurance claim; and patient needs to ensure his/her health records privacy protection while consulting with parties involved in healthcare system [1,2]. Furthermore, health records should not be perceivable to unauthorized parties with malicious intentions on the patient's health. Therefore, confidentiality, integrity, and privacy of health records should be preserved while transmitting such data over the wire and/or while storing data on a third-party server [3,4].

Cloud computing is a cost-effective computing paradigm for convenient, on-demand data access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services. In comparison to conventional desktop-based (wireless) local area networks computing paradigm, cloud computing facilitates a number of interesting features such as ubiquitous network access, on-demand service, high return-of-investment, availability of service/data, and efficient data management. Broadly, there are three types of consumers in cloud computing—Cloud server as a consumer, Merchant as a consumer, and Customer as a consumer. Cloud server facilitates storage and services, the merchant owns the application and user data which are stored in the cloud server, and the customer, registered under the merchant, gets services and access data from the cloud server [5]. Outsourcing cloud infrastructure helps application provider (e.g., merchant) and customers reducing expenditure on hardware, software, tools, and manpower. Furthermore, data access from the cloud storage anytime-anywhere makes application flexible and available to users in pay-as-you-use fashion at relatively low prices.

Blockchain technology [6] is a publicly verifiable, shared, immutable distributed ledger used for recording the history of transactions. The blockchain technology found enormous success in financial applications [7] and has potential that can reshape applications such as e-governance, healthcare, and supply-chain with respect to security, privacy, efficiency, transparency, and fault-resistance. Some interesting features that blockchain technology supports are as follows:

- **Immutability:** Immutable transaction can help in providing transparency between participants involved in the process and can be protected for modification from unauthorized entities.
- **Transparency:** The transaction in blockchain can be initiated and executed by any parties involved in the system through consensus, validation, and acceptance protocols, which makes the system transparent to its activities.
- **Verifiability:** The shared and consensus mechanism makes the executed transactions managed in blockchain technology verifiable for both insiders and outsiders.
- **Authenticity:** The transaction in blockchain typically involves digital signature of initiator and responder. In addition, use of smart contract in some applications provides transaction's authenticity.
- **Ownership:** The immutability property of transactions in block and linkability among blocks could enable ownership control as well as accountability feature in applications powered by blockchain.

With advancement of Internet technology, cloud infrastructure, machine intelligence, and blockchain technology, modern applications make digital transformation of activities aiming at better quality services to the society by a sustainable and scalable infrastructure with participatory roles and responsibilities of various stakeholders of the infrastructure. The infrastructure needs integration of several complimentary technologies, where information related to the real world and the virtual world are retrieved, combined, processed, analyzed, and distributed anywhere and anytime [8]. In addition to the conventional web of world, the convergence of mobile communication, sensors, and online social networks technologies will lead to an exponential increase in the creation and consumption of large volumes of data linked to individuals as well as society. While creating, storing, sharing, updating, disseminating and deleting a large volume of data pertaining to applications in the infrastructure, managing these data against potential adversaries is of prime concern in order to provide intended services to users of the application and beyond. Typically, data owner hires the cloud infrastructure for storing application data in the cloud storage. While resource outsourcing provides significant advantages to data owners as well as to service consumers, there are some important concerns such as security, ownership, and trust that require significant attention from research community [5,9,10]. For example, when data owners store their data in cloud server, they no longer possess their data physically. It may so happen that the cloud server manipulates the data without data owner's knowledge. In order to avoid such scenarios, data owner can store data in cloud server in an encrypted form so that cloud server cannot learn/manipulate any data in it. However, at the same time the data needs to be accessible from the cloud server by authorized consumers as per their demand [9,11].

Healthcare system with modern tools and technology is a need for societal growth. With smart and intelligent devices/services, people can connect doctor, hospital, and insurance company remotely. Numerous research results for advancing healthcare systems [1–4,11–13] have been reported in last decade. In such systems, cloud storage server as well as computing platform serves a useful intermediary to both healthcare service consumers and service providers. MediNet [1], a mobile healthcare system that can offer services to patients suffer from diabetes and cardiovascular disease. Chiarini *et al.* [4] proposed a comprehensive overview of different existing mobile health solutions chronic diseases and elders. Klasnja *et al.* [14] proposed mobile-based services for monitoring health conditions in asthma and heart diseases. Liu *et al.* [15] proposed a healthcare system, namely HealthKiosk that collects data from various biomedical sensors used for heart rate, glucose level, blood pressure, body temperature, etc. Assisted by cloud infrastructure, a few notable features that can efficiently be plugged into healthcare systems are verifiable computation, monitoring computation, computation over protected data, and availability of service from anywhere and anytime [16–23].

The usage of mobile phone in applications ranging from home appliances to consumer electronics has increased many folds by the backbone connectivity of Internet. This has not only connected applications of service providers and consumers, but also enabled a virtual human-chain through social networks and by

other means across the globe. Using the massive power of cloud, edge, and blockchain technology, one could build an application that could run on top of this as backend support, which could facilitate services with accountability, ownership, and scalability features [24–29].

In addition, controlling access to data, privacy-preservance and trust relationships are keys to convince data owners, service provider and service consumers for enabling and availing services in a desired healthcare system [16,30,31]. All entities involved in various applications such as sensors and actuators, mobile phones, data owners, and application providers require strong mechanisms for security (e.g. authentication, authorization, availability, and integrity), while managing essential trust relationships are of great importance in healthcare applications. As a result, adding a Data layer in Figure 16.1, the layered services in Figure 16.2 not only makes the service smart, but also could address transparency, accountability, and efficacy.

A data-centric distributed framework for managing the security and privacy solution for healthcare application can be devised using blockchain technology, where different servicing units could engage themselves for managing their respective activities recorded in distributed verifiable ledgers. A blockchain-powered

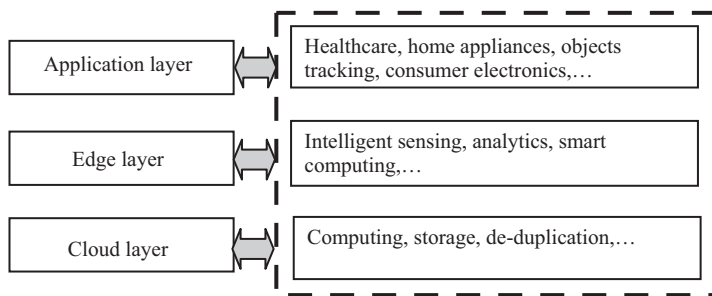


Figure 16.1 Layered services

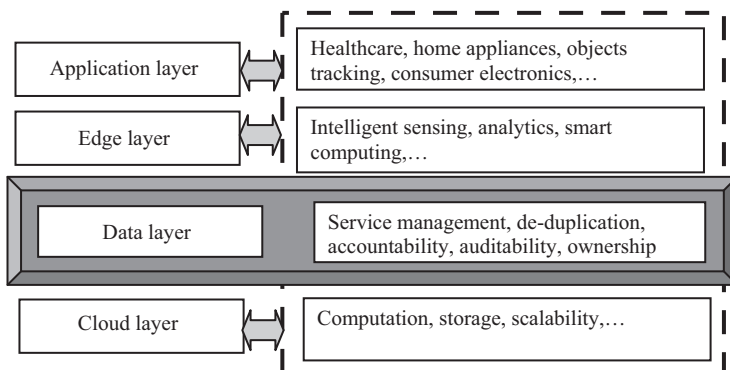


Figure 16.2 Data-powered layered services

healthcare system can make medical service transparent, accountable and auditable, where different service units can be routed through various edges which are capable of managing resource intelligently with cloud that is powered by distributed immutable and verifiable ledgers.

Our contributions: In this chapter, we discuss about the applicability of blockchain technology for protecting health records with respect to tamper-proofing, accountability, ownership, and data privacy. We present blockchain-powered protocols for securing healthcare system with emphasis on healthcare insurance of patients' data, diagnosis report, and accountability and transparency of services availed by different entities involved in healthcare system. We have devised protocols for Policy Generation, Upload Patient Reports, and Policy Claim that provides security of patient's data, diagnosis report, and accountability and transparency of services availed by participants of the system. The proposed protocols address the issue of ill-formed medical report for availing/denial of health insurance. We show how blockchain technology can address this important issue, so the patient can avail deserving service from the insurance company and the insurance company can confirm the legitimacy of the medical report.

Outline of the chapter: The structure of the chapter includes some discussion on preliminaries in Section 16.2, which can make the chapter self-content; the proposed protocols for securing healthcare insurance system is presented in Section 16.3; analysis of the proposed solutions is provided in Section 16.4; and the chapter concludes in Section 16.5.

16.2 Preliminaries

In a blockchain system, transactions are combined into blocks that form the blockchain [6], [7]. Typically, a node in the system broadcast a new transaction to all nodes, a node who finds a solution to the consensus protocols adopted in the system broadcasts the block to other nodes, the system accepts the block only if the block follows protocol rules. Finally, a chain of blocks is formed using the timestamp, hash of the accepted block, and consensus protocols that link to previous blocks. Blocks in the chain are connected to each other by referring to the hash value of the previous block. This works as a timestamp that proves that the referenced block existed at the time of creation of the block which references it. Every new block added to the chain reinforces chronological order and validity of previous blocks.

Blockchain: Blockchain is a data structure that can be publicly verifiable immutable ledger shared among distributed nodes in the system. A typical blockchain system consists of multiple nodes which do not fully trust each other. All nodes in the system agree on the transactions based on some consensus protocols and their order which cannot be modified once it gets executed. Figure 16.3 shows a typical blockchain data structure.

A blockchain system can be categorized as either public or private. In case of public blockchain system, any node can join and leave the system, and therefore,

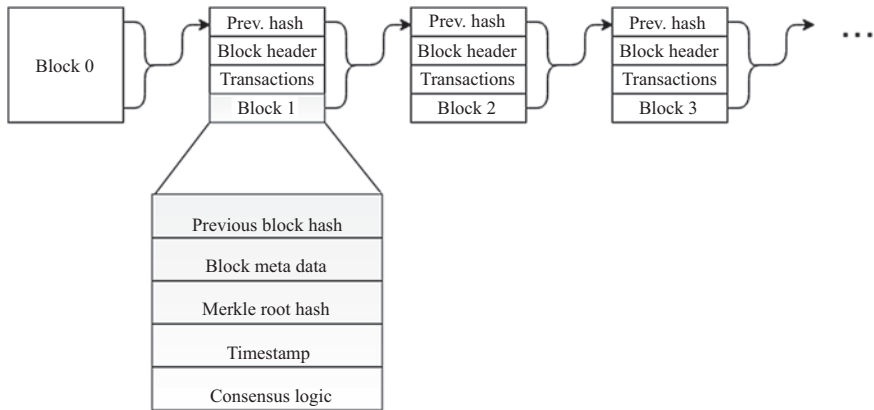


Figure 16.3 Typical blockchain structure

the blockchain is fully decentralized. In case of private blockchain system, the blockchain controls membership, who can join the system, so implicit authentication of nodes known to other nodes.

Hash function: Blockchain system uses cryptographic hash function that assures the immutability property of all transactions captured in blockchain. Out of many available hash algorithms in literature, the hash algorithms SHA-256 and RIPEMD-160 [32] are popularly used in different blockchain systems. Generally, a pseudo-random function that satisfies one-wayness and collision resistant properties can fall in the class of cryptographic hash function. One may refer to [32] for more about pseudo-random and hash function.

Hash tree: A variable number of transactions is included into a block through the Merkle tree (Figure 16.4). Transactions in the Merkle tree are hashed using secure hash algorithm (e.g., SHA256 and RIPEMD-160). A hash tree is a tree structure in which leaf nodes contain data and internal nodes are hashes of the concatenation of their child nodes. A hash tree structure is very useful to quickly check whether the existence of data or any changes occurred in some nodes.

Blockchain system makes use of hash (Merkle) tree to ensure integrity of the ledgers. For example, Hyperledger [33] uses a bucket hash tree in which states are grouped into a predefined number of buckets; Ethereum [34] uses a Patricia Merkle tree which resembles a tree and whose leaves are key-value states. The key technique adopted through the hash tree is to link the blocks through a chain of cryptographic hash pointers: the content of block number $n + 1$ contains the hash of block number n . Any modification in block n immediately invalidates all the subsequent blocks. By combining Merkle tree and hash pointers, blockchain offers a secure and efficient data model that could track all historical changes made to the block states in a blockchain system.

Digital signature: Digital signature is a cryptographic means through which the authenticity of data and source of the data, integrity of the data, and non-repudiation properties can be addressed [32]. Typically, a digital signature scheme

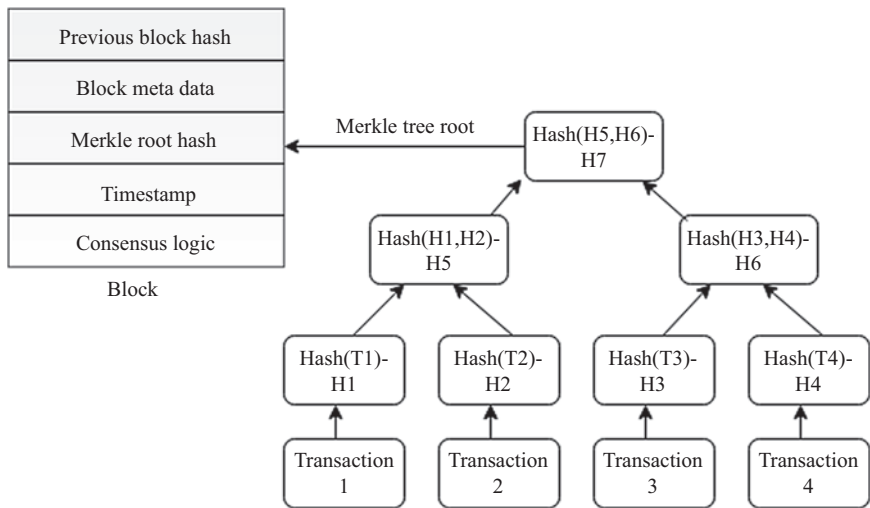


Figure 16.4 Block with Merkel root hash

is a 3-tuple (*Key Generation*, *Signature Generation*, *Signature Verification*) algorithm—the *Key Generation* algorithm inputs a security parameter and outputs the public key and private key; the *Signature Generation* algorithm inputs a message to be signed and the private key and outputs the signature on message and the *Signature Verification* algorithm inputs the signed message and the corresponding public key and outputs whether the signed message is correct or incorrect.

Consensus protocol: The content of the ledger reflects historical and current states maintained by the blockchain go through a consensus protocol agreed on by all parties in the system. Some popular consensus protocols are proof-of-work (PoW), proof-of-space (PoS), and Practical Byzantine Fault Tolerance (PBFT) [35].

Smart contract: A smart contract refers to the computation executed when a transaction is performed. It can be regarded as a stored procedure invoked upon a transaction. The inputs, outputs and states affected by the smart contract execution are agreed on by every node.

Seeing the strengths of blockchain technology which is believed to change the landscape of many applications that are controlled typically by centralized database, healthcare application is one such application that needs transparent, accountable, and auditable services which could benefit to patients, doctors, hospitals, and insurance company.

16.3 The proposed system

We present blockchain-powered protocols for securing healthcare system with emphasis on healthcare insurance of patients' data, diagnosis report, and accountability and transparency of services availed by different entities involved in

healthcare system. The proposed protocols address the issue of ill-formed medical report for availing/denial of health insurance, so that the patient can avail deserving service from the insurance company and the insurance company can confirm the legitimacy of the medical report. In particular, we focus on the trust and delay issues faced between patients and insurance company while processing a claim. In current scenario, policies are assigned manually by an insurance agent. When a patient requests for a policy, it has to provide personal information like age, health history, etc. to the insurance company. The insurance company checks whether the patient satisfies all the criteria for the policy. Later when a patient applies for claim under a certain policy, it goes through various checkpoints inside the insurance company before it gets approved or rejected. The insurance company has to verify whether medical reports submitted by the patient are legitimate and falls under the policy. Our focus is to make the claim process transparent, accountable, and auditable while preserving privacy of medical records pertaining to patients. We assume that each patient has access and control over its medical data. All medical data are uploaded by doctors or designated authority. The health insurance policies are stored in the blockchain network as a smart contract. The medical records of patients are encrypted and make the intended data available to the insurance company only when patient allows.

We proposed a solution based on a private block-chain controlled by a distributed cloud. As represented in Figure 16.5, the system has four main entities: patients, hospitals, insurance company, and the cloud. Patients are interested in availing policy service of the insurance company they have subscribed to. The insurance company has an agreement with certain group of hospitals. If a patient is treated at one of these hospitals and has a policy issued by the insurance company, then they will take care of full or partial treatment cost according to the policy

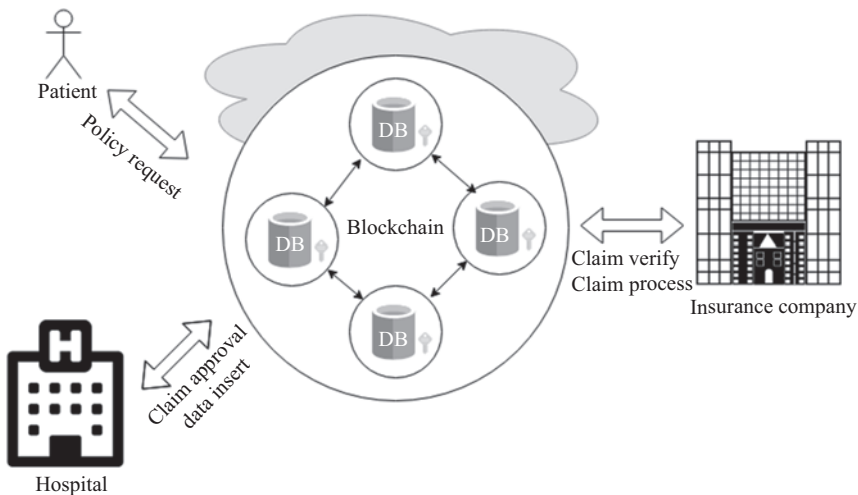


Figure 16.5 The proposed healthcare system

applicable to the patient. Hospital treats a patient and uploads patient's medical reports in cloud database and records it in the blockchain as a transaction.

The system works as follows. An insurance company puts a general smart contract S on the block-chain which is maintained by the cloud. This smart contract contains information about all the policies offered by the insurance company. Each policy has certain user eligibility criteria. If a patient fulfills those criteria for a particular policy, then only the policy is issued to the patient. Similarly, it also has eligibility criteria for claim process. At the time of claim request by a patient, smart contract verifies the information given by the patient and checks whether it is eligible for claim. A patient requests for a certain type of policy by sending required attributes like age, gender, location, etc. to the smart contract S . The smart contract S verifies eligibility criteria for the particular policy and if it satisfies all the criteria, then it generates a policy along with a policy number. It records the policy, policy number and patient's identity on the block-chain. After completion of the treatment, doctor uploads all the medical records of a patient on the cloud database in encrypted form along with signature. For each report uploaded, doctor assigns a unique consulting identification number. A patient can have multiple consulting ids. The doctor also uploads the encryption key encrypted by public key of the patient along with consulting id. It then records hash of these data on the blockchain. A report of a patient stored in the cloud database is directly accessible to the patient and corresponding doctors only. For smart contract to access these data, it requires certain parameters from the patient. For claim request, a patient sends consulting ids along with transaction ids of all the concerned data to the smart contract. It also sends the encryption key encrypted by public key of the insurance company. Using patient id and consulting ids it can access the concerned medical reports of the patient. If the medical reports satisfy all the eligibility criteria for claim, the smart contract approves for the claim; else, it rejects.

16.3.1 Description of the protocol

We use a standard symmetric encryption scheme $SE = (Key.SE; Enc.SE; Dec.SE)$, where $Key.SE$ is a symmetric key generator, $Enc.SE$ is a symmetric encryption algorithm, and $Dec.SE$ is a symmetric decryption algorithm. We also use a public key encryption scheme $PE = (Key.PE; Enc.PE; Dec.PE)$ and a digital signature scheme $DS = (Key.DS; Sign.DS; Verify.DS)$, where $Key.PE$ is a public key pair generator, $Enc.PE$ is a public key encryption algorithm, $Dec.PE$ is a public key decryption algorithm, $Key.DS$ is a public key pair generator for digital signature, $Sign.DS$ is a signing algorithm, and $Verify.DS$ is a verifying algorithm. The proposed protocols also assume an efficient cryptographic hash function H . Some notations and meaning used throughout the chapter are provided in Table 16.1.

We assume that the smart contract S is already on the blockchain and each entity of the system has a public key pair. All the public keys are stored in the cloud database. Given the identity of an entity, anyone can retrieve the corresponding public key. We also assume that detail description of each type of policy is publicly available. The proposed system is shown in Figure 16.6. The system

Table 16.1 *Notations and meaning*

Notation	Meaning
P_{id}	Patient's identity
D_{id}	Doctor's identity
C_{id}	Consulting identity for visit or treatment
IC	Insurance Company
IP	Insurance Policy
DB_I	Database of the insurance company
DB_c	Cloud database
sk	Symmetric encryption key
pk_i, pr_i	Public and private key pair of an entity i
$S \rightarrow R: m$	S sends message m to R
$S \rightarrow R: \{m\}_K$	S sends message m to R encrypted under the key K

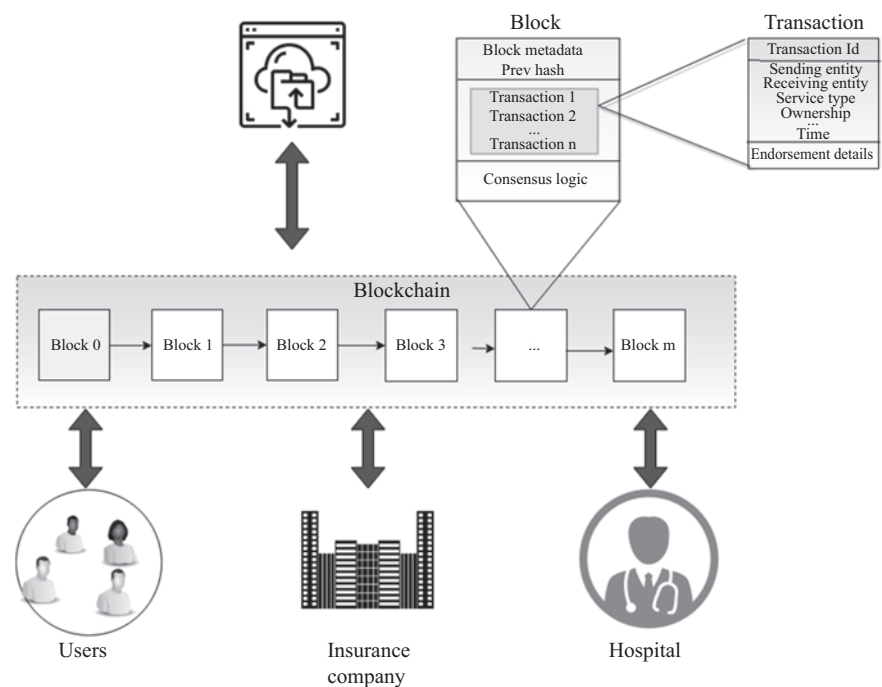


Figure 16.6 *Proposed system model*

involves mainly three protocols: *PolicyIssuanceRequest*, *UploadPatientReports*, and *PolicyClaimRequest*, as explained below.

16.3.1.1 Policy generation

A patient wants to buy a certain policy from the insurance company. Patient can look at publicly available policy descriptions and then selects a particular type of

policy. The description of each policy includes necessary attributes of a patient required for eligibility criteria. The patient sends policy type, identity P_{id} and the set A that states necessary attributes to the smart contract over blockchain. The information (Policy type, P_{id} , A) is recorded as transaction from the patient to smart contract on the blockchain. Once the smart contract receives the information, it checks whether the attribute set A is eligible for the particular type of policy. If the patient is eligible for the policy, then the smart contract creates an insurance policy IP along with a policy number PN . It records $(H(P), PN, P_{id})$ on the blockchain.

Protocol: Policy issuance request

```

procedure PolicyIssuanceRequest(Policy type,  $P_{id}$ ,  $A$ )
  //  $P_{id}$  is the identity of a patient and  $A$  is a set of attributes
  // Patient sends (Policy type,  $P_{id}$ ,  $A$ ) to the smart contract  $S$ 
   $s \leftarrow S(\text{Policy type}, P_{id}, A)$ 
  if  $s = 1$  then
    Create a new insurance policy  $IP$ 
    Generate a policy number  $PN$ 
    Store  $(IP, PN)$  on insurance companies database  $DB_I$ 
    Record  $(H(P), PN, P_{id})$  as transaction on the blockchain
  end if
end procedure

```

It is noted that no one can (including the insurance company, doctor, and patient) modify rules or terms and conditions of the policy later as it is recorded on the blockchain. This makes the claim-response process transparent and auditable if any dispute arises.

16.3.2 Medical reports uploading

Medical report uploading is required whenever a patient visits the hospital for medical check-up and/or treatments. After the completion of the treatment, all the medical reports of the patient are stored on the cloud database uploaded by the concerned doctor. Since medical reports contain sensitive information, it is necessary to encrypt this data before uploading it on the cloud. The doctor generates a random symmetric key sk and encrypts the set of reports R . It then encrypts the key sk using the public key pk_P of the patient. To provide authenticity of the data, the doctor signs the report using his/her secret key pr_D . For each visit, the doctor generates a new consulting id C_{id} . The doctor uploads encrypted data along with signature, encrypted key, doctor id, and $H(C_{id} || P_{id})$ on the cloud. It also records hash of all the uploaded data along with the consulting id C_{id} on the blockchain. Other than the patient and the concerned doctor, a person or an entity requires both the consulting id C_{id} and the patient id P_{id} to access data. This prevents an unauthorized access of the data.

Protocol: Upload patient reports

procedure UploadPatientReports(P_{id} , D_{id} , R)
 // P_{id} is the identity of a doctor and R is a set of all medical reports
 $sk \leftarrow Key.SE()$
 $E_R \leftarrow Enc.SE(sk, R)$
 $pk_p \leftarrow PublicKey(P_{id})$
 $K_p \leftarrow Enc.PE(pk_p, sk)$
 Generate a consulting id C_{id}
 Store $A = (ER, Sign.DS(pr_D, R), K_p, D_{id}, H(C_{id} || P_{id}))$ in the cloud database DB_c
 Record $(H(A), C_{id})$ as a transaction into the blockchain
end procedure

This protocol ensures patient's data privacy, authenticity of medical reports, and access control over the data. Without the help of the patient, a third party cannot access the data.

16.3.3 Policy claim against treatment

A patient request for the claim under the policy issued on his/her name is an important objective of any fair insurance policy pertaining to healthcare system. The patient first collects all the transaction ids T_i which are related to the patient's recent treatment. The transaction id contains information about consulting ids of patient's visit to a certain hospital. For each visit, the data are encrypted using a new key sk . The patient can easily retrieve the key sk from the uploaded data as the key sk is encrypted using the public key of the patient. The patient collects all the secret key sk_i of the transaction id T_i and encrypt them using public key of the insurance company. The patient sends (P_{id}, T, K) to the smart contract via a blockchain transaction.

The smart contract first checks whether there is any policy issued for P_{id} by searching the block-chain for the corresponding policy number. If there is a policy issued for P_{id} , then it checks whether the policy is still active. It follows the rest of the protocol for an active policy only. It first decrypts K and gets secret keys $\{sk_i\}_{i=1}^t$. It also parses T and gets transaction ids $\{T_i\}_{i=1}^t$. For each transaction id T_i , it gets consulting id C_{id} from the blockchain. Using P_{id} and C_{id} , the smart contract retrieves medical reports of the patient from the cloud database. It first checks the integrity of the retrieved data by verifying the hash of the data with the hash value stored on the blockchain. It then checks the authenticity of the reports by decrypting the encrypted report using the private key pr_i and then verifying the signature. For all the valid reports, it checks whether they fulfill eligibility criteria for the claim under the issued policy. If it satisfies the criteria, then it approves the claim; else, it rejects.

Here, the smart contract can easily verify the authenticity of the medical reports. Therefore, a patient cannot do any fraud for requesting the claim. For a genuine claim, the protocol automatically approves the claim and the insurance company cannot deny it.

Protocol: Policy claim request

procedure PolicyClaimRequest(P_{id} , T , K)

// T is a string of transaction id's of all concerned reports of a patient and K is a string of corresponding symmetric keys encrypted using public key of the insurance company. Upon receiving claim request, the smart contract S follows following procedure. //

```

 $s \leftarrow 0$ 
 $pr_1, pr_2, \dots, pr_t \leftarrow \text{Parse}(\text{Dec.PE}(pr_{IC}, K))$ 
 $T_1, T_2, \dots, T_t \leftarrow \text{Parse}(T)$ 
 $R \leftarrow \{ \}$ 
for  $1 \leq i \leq t$  do
   $H(A), C_{id} \leftarrow \text{BlockChain}(T_i)$ 
   $(E_R, \text{Sign.DS}(pr_D, R), D_{id}) \leftarrow \text{DB}_c(C_{id}, P_{id})$ 
   $R_i \leftarrow \text{Dec.SE}(pr_i, E_R)$ 
   $pk_D \leftarrow \text{PublicKey}(D_{id})$ 
  if  $\text{Verify.DS}(R_i, \text{Sign.DS}(pr_D, R), pk_D)$  then
     $R.append(R_i)$ 
  end if
   $IP \leftarrow \text{DB}_l(P_{id})$ 
  if  $IP(R)$  then
     $s \leftarrow 1$ 
  end if
return  $s$ 
end procedure

```

16.4 Analysis and discussions

We assume that the blockchain in the system is immutable and each involved entity manages his/her secret key in a secure manner. We also assume that the symmetric encryption scheme SE , the public key encryption scheme PE , the digital signature scheme DS , and the hash function H are all secure under standard security model of individual scheme. A malicious insurance company may deny valid claim request of a patient or it may even try to access medical reports of a nonregistered patient and a malicious user may forge the data while requesting for a claim. We show that the proposed system provides security against malicious user as well as malicious insurance company. Moreover, the system ensures patient's privacy by maintaining confidentiality of all medical reports.

A doctor uploads medical reports of a patient along with signature on cloud database in encrypted form. The signature provides authenticity of the report and the encryption prevents any third party including cloud from viewing patient's medical report. This maintains confidentiality of medical reports and provides patient's privacy. The hash of the report along with patient's consulting identity is recorded on the block-chain. Since hash of each report is stored on the block-chain, neither the hospital nor the cloud can modify reports once stored in the cloud database. Moreover, the data cannot be accessed or read by a third party without the help of the patient. This prevents unauthorized access of the data. To access a particular report, the smart contract requires the patient's id P_{id} and consulting id C_{id} of the report. If a patient is not registered with the insurance company for any policy, then the smart contract does not have the patient's id and hence cannot access any medical reports of that particular patient. This fulfills the criteria that the insurance company must not be able to access medical reports of a nonregistered patient.

We now show that the proposed scheme provides data confidentiality if PE is indistinguishability against chosen-plaintext attack (IND-CPA) secure.

Definition 1: (Data Confidentiality) *A scheme provides data confidentiality if any unauthorized entity cannot access or gain any information stored in the database.*

Theorem 1: *The proposed scheme provides data confidentiality under the assumption that the public key encryption scheme PE is IND-CPA secure.*

Proof: Given encrypted report (E_R, K_p) , an adversary's goal is to guess R with non-negligible probability. The key used for encryption R is selected at random and used only once. Therefore, E_R is equivalent to one-time pad encryption of R . Without knowledge of the symmetric key sk , an adversary cannot gain any information about R from E_R . K_p is an encryption of the symmetric key sk using public key of a patient. Let us assume that there is an adversary A who can distinguish between two records, that is, given two encrypted records (E_{R_0}, K_{0p}) and (E_{R_1}, K_{1p}) , the adversary A can guess which encrypted record is encryption of R_1 with non-negligible advantage. Let this advantage be η . We show that there exists an adversary B which can distinguish two ciphertexts encrypted under the public key encryption scheme PE with non-negligible advantage $\eta/2$.

Let sk_0 and sk_1 be two symmetric keys chosen by the adversary B and R_0 and R_1 be two reports chosen by the adversary A . The adversary A sends R_0 and R_1 to B . The adversary B sends sk_0 and sk_1 to the challenger. The challenger randomly picks $b \in \{0, 1\}$ and sends $K_{bp} = \text{Enc.PE}(pk_p, sk_b)$ to B . The adversary B encrypts R_0 with sk_0 and sends (E_{R_0}, K_{bp}) to A . The adversary A sends b^* as his guess for b to B . Since E_{R_0} is encrypted using sk_0 , the adversary A have advantage only if $b = 0$;

otherwise, it randomly guesses value of b . The adversary $\mathbf{B}$ sends b_* as guess for b to the challenger:

$$\begin{aligned}
 P[b_* = b] &= P[b_* = 0 \wedge b = 0] + P[b_* = 1 \wedge b = 1] \\
 &= P[b_* = 0|b = 0]P[b = 0] + P[b_* = 1|b = 1]P[b = 1] \\
 &= (0.5 + h)(0.5) + (0.5)(0.5) \\
 &= 0.25 + 0.5h + 0.25 \\
 &= 0.5 + h/2.
 \end{aligned}$$

Since η is non-negligible, the advantage of adversary $\mathbf{B}$ is also non-negligible. We assumed that PE is IND-CPA secure, so we arrived at a contradiction. Therefore, there does not exist any adversary who can distinguish ciphertexts with non-negligible advantage.

Each time a smart contract creates a policy, the hash value of the policy along with policy number and patient's identity is recorded on the blockchain. Once the policy is created no one can delete it until the policy gets expired. This prevents the insurance company from modifying or denying the existence of any particular policy. When a patient requests for a claim under certain policy, the insurance company may deny the claim for making financial gain. However, in the proposed system, the insurance company cannot modify the smart contract for any financial gain. Upon receiving the claim request, the smart contract follows the protocol and if the claim is valid, it automatically approves it. At the same time, the smart contract can also detect false claim easily. If a patient provides wrong data for a claim request, then the smart contract can easily check whether the data are valid and authenticated. For the claim's eligibility criteria, the smart contract considers only authenticated data uploaded on the cloud storage and recorded on the block-chain. In this way, the smart contract removes any possibility of denying true claim as well as approving false claim and builds trust between patients and the insurance company.

Definition 2: (Insurance Fraud [36]) *A insurance fraud is an act of obtaining money from an insurer for an event that did not happen by submitting forged material or data of the event.*

Theorem 2: *The proposed scheme is secure against insurance fraud if the digital signature scheme DS is unforgeable.*

Proof: Let assume that a malicious patient is successful in claiming insurance for false reports. The smart contract accepts the data only if it is stored in the cloud database along with a valid signature of a doctor. A malicious patient must need to modify existing reports in order to claim insurance for false reports. Let E_R be a valid report stored in the cloud database along with a valid signature $Sign.DS(pr_D, R)$

and a malicious patient is successful in replacing E_R with encryption of false report, $E_{R'}$. Now the smart contract approves the claim only if the signature is valid for $E_{R'}$. If a patient is able to replace $\text{Sign.DS}(pr_D, R)$ with a valid signature for R' , then the digital signature scheme DS is not secure against unforgeability. Therefore, as long as DS is unforgeable, a malicious patient cannot be successful in claiming insurance for false reports and the proposed scheme is secure against insurance fraud.

Theorem 3: *The proposed scheme is secure against valid claim rejection if the hash function H satisfies preimage resistance property.*

The smart contract is a program stored on the block-chain. A valid claim gets rejected only if either the smart contract is modified or the insurance policy of a patient is modified. The smart contract cannot be modified as the blockchain is immutable. The policy is stored in the database of the insurance company and its hash is recorded on the block-chain. If an adversary modifies the policy stored in the database, it must match with the hash recorded on the block-chain as block-chain is immutable and the adversary cannot modify the hash of the policy. Let IP be the original policy. Given IP and IP , the adversary needs to create a modified policy IP' in such a way that $IP = IP'$. If the adversary is successful in rejecting a valid claim, then the adversary is able to find a preimage for the corresponding policy, which is infeasible if the hash function H satisfies preimage resistance property. Therefore, the proposed scheme is secure against valid claim rejection if the hash function H is preimage resistance.

16.5 Conclusion

Security and privacy concerns of health records are challenging issues in healthcare systems. Patients' health records should not be perceivable to unauthorized parties with malicious intentions on the patient's health. We present protocols that address the issue of ill-formed medical report for availing/denial of health insurance. The protocols use blockchain technology that ensures accountability and transparency of services availed by different entities involved in healthcare insurance system. With the proposed protocols the patient can avail deserving service from the insurance company and the insurance company can confirm the legitimacy of the medical report. The protocols are shown secure in standard security model. The implementation of the protocols can be done in any exiting block-chain platform such as Hyperledger and Ethereum.

References

- [1] Mohan P., and Sultan S. "MediNet: a mobile healthcare management system for the Caribbean region." *Proceedings of the 6th Annual International Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous*; Toronto, ON, 2009, pp. 1–2.

- [2] Ming Y., and Zhang T. "Efficient privacy-preserving access control scheme in electronic health records system." *Journal of Sensors (Basel)*. 2018; 18(10):3520.
- [3] Ren Y., Werner R., Pazzi N., and Boukerche A. "Monitoring patients via a secure and mobile healthcare system." *Journal of IEEE Wireless Communications*. 2010; 17(1):59–65
- [4] Boric-Lubecke O., Gao X., Yavari E., Baboli M., Singh A. and Lubecke V. M. "E- healthcare: Remote monitoring, privacy, and security." *IEEE MTT-S International Microwave Symposium (IMS2014)*; Tampa, FL, 2014, pp. 1–3.
- [5] Takabi H., Joshi JBD., and Ahn G-J. "Security and privacy challenges in cloud computing environments. *Journal of IEEE Security and Privacy*. 2010; 8(6):24–31.
- [6] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. <https://news.bitcoin.com/>
- [7] Underwood S. "Blockchain beyond bitcoin." *Journal of Communications of ACM*. 2016; 59(11):15–17.
- [8] Pinno O.J.A., Gregio A.R.A., and De Bona L.C.E. "ControlChain: blockchain as a central enabler for access control authorizations in the IoT." *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM 2017)*; Singapore: IEEE, 2017, pp. 1–6.
- [9] Xiao Z., and Xiao Y. "Security and privacy in cloud computing." *Journal of IEEE Communications Surveys & Tutorials*. 2013; 15:843–859.
- [10] Vora J., Italiya P., Tanwar S., *et al.* "Ensuring Privacy and Security in E-Health Records." *Proceedings of the International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*; Colmar, France, 11–13 July 2018, pp. 192–196.
- [11] Sajid A., and Abbas H. "Data privacy in cloud-assisted healthcare systems: state of the art and future challenges." *Journal of Medical Systems*. 2016; 40(6):155.
- [12] Chiarini G., Ray P., Akter S., Masella C., and Ganz A., "mHealth technologies for chronic diseases and elders: a systematic review." *IEEE Journal on Selected Areas in Communications*. 2013; 31(9):6–18.
- [13] Kumari A., Tanwar S., Tyagi S., and Kumar N. "Fog computing for Healthcare 4.0 environment: opportunities and challenges." *Journal of Computers and Electrical Engineering*. 2018; 72:1–13.
- [14] Klasnja P., and Pratt W. "Healthcare in the pocket: mapping the space of mobile phone health interventions." *Journal of Biomedical Informatics*. 2012; 45(1):184–198.
- [15] Liu C.H., Wen J., Yu Q., Yang B., and Wang W., "HealthKiosk: a family-based connected healthcare system for long-term monitoring." *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*; Shanghai, 2011. pp. 241–246.
- [16] Bultel X., Das M. L., Gajera H., Gerault D., Giraud M., and Lafourcade P. "Verifiable private polynomial evaluation." *Proceedings of International*

- Conference on Provable Security (ProvSec 2017)*; Cham, Springer, 2017; LNCS vol. 10592, pp. 487–506.
- [17] Guo L., Fang Y., Li M., and Li P. “Verifiable privacy-preserving monitoring for cloud-assisted mHealth systems.” *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*; Kowloon, 2015; LNCS, vol. 10063, pp. 1026–1034.
 - [18] Gajera H., Naik S., and Das M.L. On the Security of “Verifiable privacy-preserving monitoring for cloud-assisted mHealth systems.” In *Proceedings of the International Conference on Information Systems Security (ICISS 2016)*; Springer, 2016. pp. 324–335
 - [19] Lin H., Shao J., Zhang C., and Fang Y. “CAM: cloud-assisted privacy preserving mobile health monitoring.” *Journal of the IEEE Transactions on Information Forensics and Security*. 2013; 8(6):985–997.
 - [20] Esposito C., De Santis A., Tortora G., Chang H., and Choo K. R., “Blockchain: a panacea for healthcare cloud-based data security and privacy?.” *Journal the IEEE Cloud Computing*. 2018; 5(1):31–37.
 - [21] Li M., Yu S., Zheng Y., Ren K., and Lou W., “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption.” *Journal of IEEE Transactions on Parallel and Distributed Systems*. 2013; 24(1):131–143.
 - [22] Gheorghe G., Asghar M. R., Lancrenon J., and Ghatpande S. “SPARER: secure cloud-proof storage for e-health scenarios.” *Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES)*; Salzburg, 2016. pp. 444–453.
 - [23] Li M., Yu S., Ren K., and Lou W. “Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings.” *Proceedings of the International Conference on Security and Privacy in Communication Systems(SecureComm 2010)*; Berlin, Heidelberg, Springer; vol. 50. pp. 89–106.
 - [24] Zyskind G., Nathan O., and Pentland A., “Decentralizing privacy: using blockchain to protect personal data.” *Proceedings of the IEEE Security and Privacy Workshops*; San Jose, CA, 2015. pp. 180–184.
 - [25] Azaria A., Ekblaw A., Vieira T., and Lippman A. “MedRec: using blockchain for medical data access and permission management.” *Proceedings of the 2nd International Conference on Open and Big Data (OBD)*; Vienna, 2016. pp. 25–30.
 - [26] Mandl K.D., Szolovits P., and Kohane I.S. “Public standards and patients” control: how to keep electronic medical records accessible but private.” *British Medical Journal*. 2001; 322(7281):283–287.
 - [27] Mertz L. “(Block) Chain reaction: a blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution.” *Journal of IEEE Pulse*. 2018; 9(3):4–7.
 - [28] Vora J., Tanwar S., Verma J. P., *et al.* “BHEEM: a blockchain-based framework for securing electronic health records.” *Proceedings of the IEEE*

- Global Communications Conference (IEEE GLOBECOM-2018)*; Abu Dhabi, UAE, December 09–13, 2018. pp. 1–6.
- [29] Vora J., Devmurari P., Tanwar S., Tyagi S., Kumar N., and Obaidat M.S. “Blind signatures based secured e-healthcare system.” *Proceedings of the International Conference on Computer, Information and Telecommunication Systems (IEEE CITS-2018)*; Colmar, France, July 11–13, 2018. pp. 177–181.
 - [30] Yao X., Lin Y., Liu Q., and Zhang J. “Privacy-preserving search over encrypted personal health record in multi-source cloud.” *Journal of IEEE Access*. 2018; 6:3809–3823.
 - [31] Benaloh J., Chase M., Horvitz E., and Lauter K. “Patient controlled encryption: ensuring privacy of electronic medical records.” *In Proceedings of ACM Workshop Cloud Computing Security (CCSW’09)*; Chicago, IL, USA 2009. pp. 103–114.
 - [32] Menezes A.J., Katz J., van Oorschot P.C., and Vanstone S.A. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press; 1996.
 - [33] Hyperledger. The Linux Foundation Project. <https://www.hyperledger.org/>
 - [34] Ethereum. <https://www.ethereum.org/>
 - [35] Croman K., Decker C., Eyal I., *et al.* “On scaling decentralized blockchains.” *In Proceedings of International Conference on Financial Cryptography and Data Security*; Berlin, Heidelberg, Springer, 2016. pp. 106–125.
 - [36] Derrig R.A. “Insurance fraud.” *Journal of Risk and Insurance*. 2002; 69(3): 271–287.

This page intentionally left blank

Chapter 17

Conclusion

Sudeep Tanwar¹, Sudhanshu Tyagi², and Neeraj Kumar³

This book addressed one of the most overlooked practical, methodological, and moral problems of any nation to maintain privacy and security in the healthcare sector. For example, following questions need to be addressed in this domain. Who can access the information on user electronic health record (EHR) and how can users see the information in their record to ensure the correctness? How is it protected from loss, theft, and hacking? What should users do if they think their information is compromised? In this book, we discussed a detailed framework to maintain security and privacy in electronic healthcare records, and comparative case studies using various performance evaluation metrics, such as privacy preservation, scalability, and healthcare legislation.

Service providers in Healthcare must ensure that the mechanisms for the security stand in place to counter unapproved access and data gaps. Patients should have knowledge about their data management system. EHRs enable organized medical information to be shared among authorized caregivers so as to boost the standard of health care delivery. In these systems, safety and privacy considerations are crucial because the patient may have serious issues, if sensitive data is altered. In this book, we explored a set of privacy and safety system which necessities the use of cloud platform in healthcare information sharing based on literature survey and the multi-sided safety analysis approach in the scenario-driven strategy.

The security issues are inevitable for the health information in EHR environment. Within the industry, analogous security implementations allow personal convenience and the access of specific patient's electronic health records from a selection of locations without compromising the data security. Though electronic medical records can't provide safety instances of security breach, but still the implementation of protocols for electronic systems provides better security in comparison to the safety measures which are used in analogous manual systems.

¹Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmadabad, India

²Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala, India

³Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, India

Moreover, EHR affects the protections mechanisms which we want to retain because user's health information's is confidential.

To establish the trust between the caregiver's, use of EHR is also explored in this book. It gives a methodical analysis of many features to the end users well-being care exercise to classify the weaknesses in the security level, if found any. The negligence for safety practices among the medical staff is one of the biggest threats for the EHR security. A recent study conducted in Spain shows that a miserable state of EHR security, where around 45% of state hospitals do not have standard EHR system with them and more than 30% of public hospitals do not have methods in place to avoid unauthorized access to EHR. The total number of hospitals which do not possess a safety audition for their EHR is about 66%. Centralized American and European EHR systems can turn into a certainty in the near future. Therefore, to handle the aforementioned issue, in this book, various security control methods are discussed which are defined for the EHR system having real-time challenges.

A centralized server, which receives and keeps the EHRs from various hospitals make the EHR data easily accessible to all caregivers, but it also increases the danger of exposing the health data or distributing it to the unauthorized personals. So, privacy and safety issues are thus becoming even more significant in such a multiorganizational environment. Major acceptance of the updated cloud platform facilitate the developments in healthcare, a limitation in context with safety and privacy issues. In cloud-based EHRs, the bulk of security techniques use service-oriented architecture in which services can be accessed by using the web servers. Moreover, for PHR deployment, a hybrid cloud is used, but the challenge is to preserve a secure mechanism for the construction of personal healthcare records (PHR) system. This book also explored current enforced or planned PHR schemes which have integrity, reliability, and cloud-based service. Moreover, the major analysis areas are classified as systems standards, integration, developed systems, privacy and security, and PHR recommendations for EHR development.

EHR systems can lead the on-going healthcare revolution conferring to the healthcare system's structural, procedural, and technical model changes, thus meeting the necessities and prospects of domain-specific medical staff including the patients. Despite all progress in data-driven answers, a secure scheme needs to be designed for the modeling of the electronic health records, where medical personals define all the requirements, base perceptions, associations, etc.

In future, we will explore various applications where Blockchain can be a viable solution to maintain the security and privacy of the end users. We will also explore what are the various data storage techniques which can be applicable for the efficient retrieval of the information from different locations across the globe which will give insights to the readers to apply one of the techniques in comparison to its merits over the others.

Index

- access control 10–12, 50, 81, 85,
100–1, 107, 201
 - attribute-based access control
(ABAC) 101, 196
 - contextual role-based access
control 231–3
 - criticality aware access control
(CAAC) 208–9
 - cryptographic access control 101–2
 - discretionary access control (DAC)
82
 - high level seven (HL7) role-based
access control model 195–6
 - information access control: *see*
information access control
 - mandatory access control (MAC) 82
 - privacy access control model 196–7
 - role-based access control (RBAC)
10, 76, 82, 101, 191–4, 208,
230–1
 - task role-based access control
model 194–5
 - technical aspects of 77–8
- access control list (ACL) 30, 71
- access management 71
 - activities 74
 - assets 76
 - components 75
 - identity status, monitoring 75
 - logging and tracking access 75
 - privileges 76
 - providing rights 74–5
 - requesting access 74
 - role 76
 - threats to access management 77
 - users 75
 - verification 74
 - application owner 74
 - components 75
 - definition 71
 - elements of 72
 - employee manager 74
 - external customer and partner 73
 - internal employee 73
 - IT administrator 73–4
 - objective of 72
 - “role” in 76
 - scope of 72
 - security architect 72–3
 - techniques 82
 - discretionary access control
(DAC) 82
 - mandatory access control (MAC)
82
 - role-based access control
(RBAC) 82
 - threats to 77
 - see also* identity and access
management (IAM)
- access privileges 79, 171, 307, 330
- access request 74
- access right management 80
- accountability 211
 - attribute-based signatures (ABS)
211–12
- actors in EHR system 96
- address resolution protocol (ARP)
spoofing attack 163
- advanced Block-Chain (ABC)
approach 326
- advantages of EHR system 7, 47–8
 - convenience 7
 - enhanced quality of care 7
 - saving efforts and time 7–8

- algebraic signatures 205–6
- altering patient information 54
- anonymization 237
- anonymous signatures 104
 - group signature 104–5
 - ring signature 105
- application owner 74
- application security 29
- architecture-based identification 65
- artificial intelligence (AI) 3, 321
- assets in user-management 76
- attacks over EHR 162
 - denial of service 162
 - destruction and modification 162
 - disclosure 162
 - insider attack 162–3
 - masquerading 162
 - repudiation 162
 - spoofing attack 163
- attribute-based access control
 - (ABAC) 10, 101–2, 196–7
- attribute-based encryption (ABE) 103,
155, 157, 165–6, 209–10
 - hierarchical 168
 - multiauthority 166–7
- attribute-based encryption scheme
(ASBE) 168–70
- attribute-based signatures (ABS)
211–12
- attribute disclosure 239–40
- attribute set based encryption 157,
168–71
- audit 81
- audit trail 11, 28, 32, 39, 49–50
- authentication 64, 66, 80, 87, 200,
213, 335
 - and access for health data 306–7
 - comparison of authentication
schemes 174
 - definition 66
 - device authentication 215
 - digital watermarking 213
 - discrete cosine transformation 213
 - discrete Fourier transformation
(DFT) 213
 - frequency domain 213
 - image data authentication 213
 - multiserver identification
 - techniques 66–70
 - analysis of 70
 - Lee et al. scheme 67–8
 - Leu et al. scheme 69
 - Li et al. scheme 68
 - Xue et al. scheme 68–9
 - spatial domain-based digital image
embedding 214
 - stenography 214–15
 - in wireless sensor network (WSN)
202
- authentication and authorization
(A&A) 28–9, 64
- authorization 28, 31, 64, 71
 - definition 71
- availability 98, 161, 353
 - data availability 31–2
- benefits of EHR technology 8
- BHEEM framework 38
- big data, security model for healthcare
in 200
 - access control 201
 - authentication 200
 - data encryption 200–1
 - data masking mechanism 201
 - monitoring and auditing 201
- biometric-based authentication 31,
174
- biometrics 31, 78
- BLOB files 277–8
- blockchain 111, 321, 373–4
 - advantages of using 114
 - anonymity 115
 - decentralized management 114
 - immutable records 115
 - nonrepudiation 115
 - robustness/availability 115
- centralized architectures, problems
with 113
- interoperability and
fragmentation 113

- problems with data sharing
 - 114
- security and privacy issues
 - 113–14
- challenges 117, 331
 - communication scalability-based
 - healthcare systems 333
 - data privacy and protection
 - 332
 - data storage requirements 332
 - design improvements 332
 - identification and confidentiality
 - 117–18
 - key management 118–19
 - possible attacks 118
 - scalability 118
- consensus algorithms 116–17
- future research directions 341–2
- identity and claims 121
 - application for EHR systems
 - 125
 - decentralized identifiers (DID)
 - 122
 - Sovrin, working of 123–5
 - verifiable credential 122–3
- implementation 115–16
- MedRec distributed ledger system
 - 119–20
- potential uses in healthcare
 - industry 338
 - digital identification of the
 - patient 340
 - flexible data exchange between
 - parties 339
 - insurance claims
 - reimbursements 341
 - learning ecosystem development
 - for decision making 340
 - patient controlled healthcare
 - services 339–40
 - prescription and supply tracking
 - of narcotics drugs 339
- for privacy protection 38
 - homomorphic encryption 38
 - state channels 39
- public and permissioned
 - blockchains 116
- scope for tightening security offered
 - by 333
 - authentication 335
 - consensus model 335
 - distributed consensus-based on
 - network scenario 335
 - Ethereum 336–8
 - Hyperledger 338
 - smart contracts 117
 - storing data off chain 120–1
 - working 324–6
- blockchain, enhancement of health-
 - care services using 345
- future trends 365–6
- health-care blockchain 359
 - benefits of 362–4
 - challenges of 364–5
- history of concerning issues 347
 - blockchain life cycle, transaction
 - of 350–1
 - blockchain technology, history
 - of 349
 - data protection, history of 349
 - health care, history of 348–9
 - traditional health-care system
 - 347–8
 - transform lives, ability to 352
- laws of privacy 346–7
- system design 352
 - cloud services 357–8
 - distributed network 353–5
 - doctors 356
 - health-care industry 357
 - insurance agency 358
 - Internet service provider 357
 - patients 355–6
 - pharmaceutical industry
 - 358–9
 - security principle 352–3
- blockchain-based health information
 - privacy protection 305
- authentication and access for health
 - data 306–7

- case studies 307
 - design and implementation 309
 - EHR centralized systems with security control 309–10
 - EHR privacy of sensitive information 310
 - knowledge of background 308
 - local problems with planned improvement 309
 - process on technology evaluation 311
 - risk assessment for EHR HIPAA 311
 - surveillance program of EHR 310
- healthcare, blockchain in 306
- healthcare IT systems 313
 - current privacy in healthcare IT systems 313
 - IT security challenges and case studies 313–15
 - technical solutions to secure privacy 313
- health information 306
- health-related data privacy 306
- laws, policies, and standards 311
 - practical examples of privacy policies 311–12
 - privacy legal protection with laws 311
 - standards in the area of privacy and security 312–13
- participants in healthcare and e-healthcare 306
- protection and recover for health data 307
- solutions 315
 - blockchain impact 315
 - performance evaluation metrics for security and privacy 316–17
 - technological frameworks 316
 - storage and maintenance in health data 307
- blockchain integrated healthcare data management system 326–31
 - blockchain-powered healthcare insurance system 369
 - analysis and discussions 381–4
 - proposed system 375
 - description of the protocol 377–9
 - medical reports uploading 379–80
 - policy claim against treatment 380–1
 - blockchain work 317
 - Bluetooth technology 134
 - body sensor network (BSN) 334
 - bookkeeping of disclosures 55
 - break the glass (BTG) policy 229
 - “Break-the-Glass” 237, 310
 - Business Associates (BAs) 50–1
 - Business to Business (B2B) 72
 - Business to Consumers (B2C) 72
 - Business to Employee (B2E) 72
 - Byzantine Fault Tolerant Algorithms 117
 - The California Online Privacy Protection Act (CalOPPA) 346
 - Catch Me (If You Can) mechanism 206
 - CCHIT (Certification Commission for Healthcare Information Technology) certification 37
 - centralized architectures, problems with 113
 - data sharing, problems with 114
 - interoperability and fragmentation 113
 - security and privacy issues 113–14
 - centralized identity management 82
 - centralized server 390
 - centralized system 10, 353–4
 - certificate authority (CA) 82
 - Certification Commission for Healthcare Information Technology (CCHIT) 254
 - challenges in EHR adoption 24
 - data completeness and correctness 26–7

- financial challenge 24–5
- integration with other systems 25
- interoperability 25
- personnel cooperation 25
- privacy concerns 28–9
- security of EHR data 27–8
- storage of EHR data 27
- technological makeover 24
- usability 25–6
- characteristics, EHR 251
- chemical sensors 139–40
- ciphertext policy attribute-based
 - encryption (CP-ABE) 102–3, 157, 165, 210
- “claimant” 65
- clinical document architecture (CDA) 97
- clinical history (CH) 267
- cloud 357–8
 - advantages of 105–6
 - application implemented completely in 275–9
 - based electronic record systems 107
 - integration 110–11
 - storage and usage 111
- cloud computing (CC) 3, 158–60, 370
 - security model for healthcare in 198–200
- communication scalability-based
 - healthcare systems 333
- communication technologies 3
- components of EHR 22
 - additional desirable capabilities 23–4
 - core components of an EHR 22–3
- Computerized Physician Order Entry (CPOE) 25, 252–3
- confidential attributes 239
- confidential communications, ideal to 55
- confidentiality 48–50, 204–5, 225, 314, 353
 - defined 98
 - integrity and 12
 - preserving 31
 - privacy and 48–9
- confidentiality, integrity, and
 - availability (CIA) 98, 184, 186
- connected/tethered PHRs 5
- consensus model 335
- consensus protocol 118, 375
- consistency (Co) 26
- contextual role-based access control 231–3
- core components of an EHR 22–3
- Covered Entities (CEs) 50
- credential issuance and management 80
- credential system 173
- criticality aware access control (CAAC) 208–9
- cryptographic access control (CAC)
 - model 10, 101–2
- cryptographic-based keying material (CKM) 209
- C-TMAC model 198
- customization of EHR 261
 - efficiency 261
 - emergency 262
 - organization of data 261–2
 - personalization 261
- data access security 208
 - criticality aware access control (CAAC) 208–9
- data sharing security 212
- public key cryptography (PKC) 209
 - accountability 211–12
 - attribute-based encryption (ABE) 209–10
 - ciphertext policy-based ABE (CP-ABE) 210
 - hybridized CP and KP-based ABE (CP-KEM-ABE) 211
 - key policy-based ABE (KP-ABE) 210–11
- role-based access control (RBAC) 208

- symmetric key cryptography (SKC) 209
- data availability 31–2
- database management system (DBMS) 140
- data breach and mandatory disclosure 32–3
- data completeness and correctness 26–7
- data confidentiality 164, 171, 174, 382
- data control 12, 50, 208
- data encryption 100, 102, 107, 200–1
- Datagram Transport Layer Security (DTLS) 83
- data integrity 31, 160
- data masking mechanism 201
- data mining 26, 190
- data ownership 189
- data privacy 36, 157, 161, 323, 334
- data security in healthcare 184–6
- data security policies 12, 50
- data sharing 6
 - problems with 114
 - security 212
- data storage 189
 - requirements 3332
 - unencrypted 107
- data storage security 204
 - algebraic signatures 205–6
 - Catch Me (If You Can) mechanism 206
 - confidentiality 204–5
 - dependability 205
 - integrity 205
 - redundant residual number systems (RRNS) 205
 - threat analysis 206
 - information threats 207–8
 - intentional threats 207
 - natural threats 206–7
 - network threats 207
 - transmission threats 207
 - unintentional threats 207
- data type 189
- decentralized identifiers (DID) 122
- default IDs and passwords 87
- Delegated Proof of Stake 117
- dependability 205
- depersonalization 237
- destruction and modification attack made 162
- development of EHR systems 99
 - access control 100
 - attribute-based access control (ABAC) 101
 - cryptographic access control 101–2
 - role-based access control (RBAC) 101
- compliance 99–100
- digital signature and verification 104
 - anonymous signatures 104–5
 - threshold signatures 105
- encryption techniques 100
- identity-based encryption 102
 - ciphertext policy attribute-based encryption (CP-ABE) 102–3
 - key policy attribute-based encryption 103
- key management 103–4
- device authentication 215
- Diffie–Hellman key agreement (DH-KA) 164
- digital certificate 124
 - login/password with 173
- digital signature 104, 374–5
 - anonymous signatures 104
 - group signature 104–5
 - ring signature 105
- schemes 173
- threshold signatures 105
- digital watermarking 213
- disasters, alerts for 143
- disclosure 55, 162
 - accidental 226
 - risk 229
 - statistical disclosure control 229–30

- discrete cosine transformation 213
- discrete Fourier transformation (DFT) 213
- discretionary access control (DAC) 82
- distributed denial of service (DDoS) 98, 117
- distributed network 353
 - centralized system 353–4
 - distributed system 354–5
- distributed system 354–5
- doctors 7, 9, 48, 164, 230, 355–6
- domain name system (DNS) server
 - spoofing attack 163
- Effective Information Presentation (EIP) 26
- Effective Use of Language (EUL) 26
- Efficient Interactions (EI) 26
- eHealth and teratology 262
- E-health-care models, generalizing 55–6
- e-healthcare service, privacy access
 - control model for 196–7
- e-health care system, implementation
 - components for 85
 - administering IDs 86
 - authentication 87
 - default IDs and passwords 87
 - enforcement 88
 - general access controls 85–6
 - human resource considerations 85
 - privileged IDs 86
 - remote access 87–8
 - service ID 86
 - session management 88
 - sign-on controls 87
- Electronic Protected Health Information (ePHI) 36
- electronic record (eRecs) 233–4
- elliptic curve cryptography (ECC) 83
- employee manager 74
- encrypted data 107
- encryption mechanism in wireless
 - sensor network (WSN) 202
- encryption technique 100, 191
- enforcement 88
- Enhanced Medical Information Security (EMIS) 310
- ensured wellbeing data 51
- enterprise, impact on 285
- entity-based identification 65
- eRecs 233–4
- eTags 233–4
- Ethereum 336
 - account 336–8
 - architecture 336
- Ethereum Virtual machine (EVM) 336
- evidence-based tools 6
- external customers and partners (ECP) 73
- fault-tolerance systems 31
- federated identity management (FIM) 81
- financial challenges in adopting EHR 24–5
- fine-grained access control 103, 111, 120, 161, 168, 171
- fog computing 160
- Forgiveness and Feedback (FoF) 26
- frequency domain 213
- functionalities of EHR system 23
- gas sensors 137
- global health security 188
- global identifier (GID) 167
- Government of India initiative toward EHRs 22
- group signature 104–5
- hacking 31
- handheld devices networks versus IoT networks 144
 - network scalability in heterogeneous environment 144–5
 - required long battery life 144
 - required low deployment and adaptability cost 145–7
- handheld devices' role in IoTs 143–4
- handwritten prescriptions 18–19

- ul style="list-style-type: none;">
- hash function 67, 335, 338, 374, 384
- hash tree 374
- hazard capacity method for breaches
 - 53
 - examination and enforcement of potential ACT violations 53–4
 - revealing breaches 53
 - understanding patients' health information rights 54–5
- Health and Human Services (HHS) 38, 52
- Healthcare 1.0 3
- Healthcare 2.0 3
- Healthcare 3.0 3
- Healthcare 4.0 4
- healthcare evolution 186–7
- healthcare industry 3, 93, 119, 288, 357
 - revolution in 3–4
- Healthcare Information and Management Systems Society (HIMSS) 26
- healthcare information systems (HISs) 187, 208, 214, 224
- healthcare IT systems 313
 - current privacy in healthcare IT systems 313
 - IT security challenges and case studies 313–15
 - technical solutions to secure privacy 313
- health-care system, fundamentals of 43–4
 - advantages of EHR system 47–8
 - current scope of research 56
 - generalize E-health-care models 55–6
 - hazard capacity method for breaches 53
 - examination and enforcement of potential ACT violations 53–4
 - revealing breaches 53
 - understanding patients' health information rights 54–5
 - HIPAA rules 50
 - breach notification rule 52–3
 - privacy rule 51
 - security rule 52
 - privacy and security concern, scratch for 48
 - health information privacy and security, background of 48
 - privacy and confidentiality 48–9
 - problems arise in security and privacy 49–50
 - security 49
 - traditional medical care system, workflow of 44–5
 - workflow of EHR systems 45–7
- Health Information Exchange (HIE) 22
- health information privacy, case studies in 307
 - design and implementation 309
- EHR centralized systems with security control 309–10
- EHR privacy of sensitive information 310
- knowledge of background 308
- local problems with planned improvement 309
- process on technology evaluation 311
- risk assessment for EHR HIPAA 311
- surveillance program of EHR 310
- Health Insurance, Portability and Accountability Act (HIPAA) 5, 24, 33, 50, 99, 160, 190–1, 203
 - breach notification rule 52–3
 - privacy rule 51
 - security rule 52
- Health Level Seven (HL7) 268
- Health Monitoring and Risk Evaluation of Earthen Sites (HMRE2S) model 143
- health-related data privacy 306

- health security as a public health
 - concept 188
- hierarchical attribute-based
 - encryption 168
- hierarchical attribute set based
 - encryption (HASBE) 170–1
- hierarchical identity-based encryption (HIBE) 109
- high level seven (HL7) role-based
 - access control model 195–6
- HITECH (Health Information Technology or Economic and Clinical Health) Act 33, 37
- HL7 V3 standard 97
- homomorphic encryption 38
- hospital information system (HIS) 4
- humidity sensors 136–7
- hybridized CP and KP-based ABE (CP-KEM-ABE) 211
- hybrid public key infrastructure (HPKI) 100
- Hyperledger 335, 338, 374
- identification 61, 64–6
 - architecture-based 65
 - definition 64
 - entity-based 65
 - life-cycle of 62
 - process-based 65–6
 - something inherent 65
 - something known 65
 - something possessed 65
 - types of identification techniques 65
- identifier attributes 239
- identity and access management (IAM) 71, 77
 - access privileges not changing
 - commensurately with internal role changes 79
 - biometrics 78
 - deletion of test accounts after usage 79
 - e-health care system,
 - implementation components for (case study) 82, 85
 - administering IDs 86
 - authentication 87
 - default IDs and passwords 87
 - enforcement 88
 - general access controls 85–6
 - human resource considerations 85
 - privileged IDs 86
 - remote access 87–8
 - service ID 86
 - session management 88
 - sign-on controls 87
- human factor 77
- IoT-based healthcare security 82–4
- multifactor authentication 78
- poor management of processes 78
- remote access solutions 78
- single sign-on 78
- smart e-health gateway 84
- technical aspects of access control 77–8
- user account creation without any approval 78–9
- identity-based encryption (IBE) 102, 165
 - ciphertext policy attribute-based encryption (CP-ABE) 102–3
 - key policy attribute-based encryption 103
- identity disclosure 239–40
- identity management techniques 81
 - centralized identity management 82
 - federated identity management (FIM) 81
 - isolated identity management 81
- identity status, monitoring 75
- IDs
 - administering 86
 - default IDs and passwords 87
 - privileged 86
 - service 86
- image data authentication 213
- information access control 227–30
 - contextual role-based access control 231–3

- privacy management architecture 235–7
- role-based access control (RBAC) 230–1
- tag-based data model 233–5
- information communication
 - technology (ICT) 4
- information flow 290–2
- information loss 229
- information security and privacy in
 - healthcare records 223
 - future directions 242–4
- information access control 227–30
 - contextual role-based access control 231–3
 - privacy management architecture 235–7
 - role-based access control (RBAC) 230–1
 - tag-based data model 233–5
- statistical disclosure control 229–30, 237
 - microaggregation 241–2
 - p-sensitive k-anonymity property 239–41
 - pseudonymization 237–9
- threats to 225
 - organizational threats 226
 - systemic threats 227
- information security management (ISM) 75
- information security management system (ISMS) 63
- information threats 207–8
- infrared thermography (IRT) 142
- insider attack 162–3
- insurance agency 358
- insurance fraud 383
- Integrated Health Information Platform (IHIP) 22
- integration of EHR with different other systems 25
- integrity 98, 205, 353
 - and confidentiality 12, 50
 - data integrity 31, 160
- intentional threats 207
- internal employee 73
- International Telecommunications Union (ITU) 135
- The International Telecommunication Union (ITU)
 - Telecommunication Standardization Sector (ITU-T) 62
- Internet of thing (IoT) 3, 66, 227, 334, 349
- Internet of things (IoTs) services with
 - touch-enabled handheld devices 131
- diverse solutions, IoT architecture for 135–41
- emerging IoT technologies 133
 - Bluetooth technology 134
 - low power wide area network (LoRaWAN) 135
 - Wi-Fi (wireless fidelity) technology 134
 - Zigbee 134–5
 - Z-wave 135
- future scope 148
- handheld devices' role in IoTs 143–4
- IoT-based healthcare security 82–4
- opportunities and challenges of
 - IoTs with handheld devices 147–8
- real-world application areas 141
 - disasters, alerts for 143
 - healthcare 141–2
 - logistics and supply chain management (SCM) 142–3
 - smart agriculture 143
 - smart home/office/buildings 142
 - transportation 143
 - wearable 142
- versus handheld devices networks 144
 - network scalability in heterogeneous environment 144–5
 - required long battery life 144
 - required low deployment and adaptability cost 145–7

- Internet service provider 357
- interoperability 25, 160
 - and fragmentation 113
 - and open systems 96–7
- IP address spoofing attack 163
- isolated identity management 81
- ISO standards for security 62
 - ISO/IEC 27001 standard 63
 - ISO/IEC 9798 63
 - ISO/TC 215 standards 312
- IT administrator 73–4
- k-anonymity property 239–40
- key ABE (KP-ABE) 165–6
- key attributes 239–40
- keying material (KM) 209
- Key Management Interoperability Protocol (KMIP) 276
- key management system 103–4
- key policy attribute-based
 - encryption (KP-ABE) 103, 157, 210–11
- key variables 241
- KLAS studies 255
- laws, policies, and standards 311
 - practical examples of privacy policies 311–12
 - privacy legal protection with laws 311
 - standards in the area of privacy and security 312–13
- least significant bit (LSB) 214
- light weighted digital certificate (LDC) 209
- logging and tracking access 75
- login/password with digital certificate 173
- long pursuit, storing and preserving the storage of records for 258
- low power wide area network (LoRaWAN) 135
- machine–machine (M2M)
 - communication 132
- mandatory access control (MAC) 82
- mandatory safety for EHR in an organization 251–2
- MarkLogic9 288
- masquerading 162
- medical data breach 32, 256–7
- medical data processing by a professional 270–1
- medical record maintenance 254
 - achieving performance in EHR using safety testing and reporting mechanism 255
 - implementation and design of safe EHR 254–5
 - managing and preventing EHR-related flaws 255–6
- MedRec system 119–20, 176
- Merkle tree 374
- microaggregation 241–2
- Minimize Cognitive Load (MCL) 26
- minimum sum of squares clustering (MSSC) problem 242
- Ministry of Health and Family Welfare (MoHFW) 22
- misuse of health record 13, 50
- MiT M (Man in the middle attack) 30
- mock drills 32
- models for healthcare security 191
 - attribute role-based access control (ABAC) model 196
 - HIPAA privacy rules 203
 - HL7 role-based access control model 195–6
 - privacy access control model for e-healthcare service 196–7
 - role-based access control model (RBAC) healthcare model 192–4
 - security model for healthcare in big data 200
 - access control 201
 - authentication 200
 - data encryption 200–1
 - data masking mechanism 201
 - monitoring and auditing 201
 - security model for healthcare in cloud computing 198–200

- security model for healthcare in
 - wireless sensor network 201–2
 - authentication mechanism 202
 - encryption mechanism 202
- task role-based access control
 - model 194–5
- TMAC model 197
 - C-TMAC model 198
 - T-TMAC model 198
- monitoring and auditing 201
- Most Significant Bit (MSB) 214
- motion sensors 138
- moving toward EHR 19–22
- multiauthority ABE 157
- multiauthority attribute-based
 - encryption 166–8
- multidimensional α secure key
 - establishment (M α SKE) mechanism 209
- multifactor authentication 78
- multiserver identification techniques
 - 66–70
 - analysis of 70
 - Lee et al. scheme 67–8
 - Leu et al. scheme 69
 - Li et al. scheme 68
 - Xue et al. scheme 68–9
- NAS (Network Attached Storage) 30
- naturalness (Na) 26
- natural threats 206–7
- network communication issue 5
- network scenario, distributed
 - consensus-based on 335
- network threats 207
- NIST approach 258–9
- NoSQL data platform 288
- ONC (Office of the National Coordinator for Health Information Technology) 37
- one-time key (OTA) 204
- openEHR 97
- Optical Character Recognition (OCR)
 - 52–3
- organizational threats 226
- organization-centered e-HIS 313
- OTP (one-time password) 31
- owner of patient data 34–5
- paper-based health records (PBHR)
 - 156
- paper-based records 18–19
- password constraints 31
- password/PIN 173–4
- patient data, owner of 34–5
- “Patient Highlights” 310
- patients 355–6
- periphery security 30
- personal data, prohibition of processing
 - of 269–70
- personal health record (PHR) 4, 107
 - privacy and security issue in
 - accidental disclosure 5
 - insider curiosity and subordination 5
 - outsider intrusion 5
 - uncontrolled secondary usage 5–6
- personal information (PI) 9, 36
 - framework for the protection of, in the healthcare context 269
- The Personal Information Protection and Electronic Documents Act (PIPEDA) 346
- personnel cooperation 25
- person/patient-centered HIS 313
- pharmaceutical industry 358–9
- physical security 29
- physicians using the EHRs 7
- prediction disclosure 241
- Preservation of Context (PC) 26
- pressure sensors 137
- privacy, defined 28
 - in healthcare settings 28–9
- privacy access control model for
 - e-healthcare service 196–7
- privacy and confidentiality 48–9
- privacy and related risks, identifying
 - 292–4

- privacy and security concern, scratch for 48
 - health information privacy and security, background of 48
 - privacy and confidentiality 48–9
 - problems arise in security and privacy 49–50
 - security 49
- privacy and security in healthcare 93
 - blockchain for EHR systems 111
 - blockchain overview 114–19
 - identity and claims 121–5
 - MedRec distributed ledger system 119–20
 - problems with centralized architectures 113–14
 - storing data off chain 120–1
 - EHR system framework 105
 - advantages of cloud 105–6
 - cloud-based electronic record systems 107–11
 - organization of EHR frameworks 106–7
 - solutions for EHR development 99
 - access control 100–2
 - compliance 99–100
 - digital signature and verification 104–5
 - encryption techniques 100
 - identity-based encryption 102–3
 - key management 103–4
 - understanding EHR systems 94
 - actors in EHR system 96
 - requirements from electronic health system 96
 - structure of EHR 95–6
- privacy and security in healthcare records 183
 - algorithms for security and privacy of healthcare system 203–4
 - authentication 213
 - device authentication 215
 - digital watermarking 213
 - discrete cosine transformation 213
 - discrete Fourier transformation (DFT) 213
 - frequency domain 213
 - image data authentication 213
 - spatial domain-based digital image embedding 214
 - stenography 214–15
 - conflicting regulatory framework 190
 - authentication mechanisms 191
 - encryption technique 191
 - role-based access control model (RBAC) 191
 - data access and storage 188
 - data ownership 189
 - data storage 189
 - data type 189
 - viewers of patient's medical records 190
 - data access security 208
 - criticality aware access control (CAAC) 208–9
 - data sharing security 212
 - public key cryptography (PKC) 209–12
 - role-based access control (RBAC) 208
 - symmetric key cryptography (SKC) 209
 - data mining 190
 - data security in healthcare 184–6
 - data storage security 204
 - algebraic signatures 205–6
 - Catch Me (If You Can) mechanism 206
 - confidentiality 204–5
 - dependability 205
 - integrity 205
 - redundant residual number systems (RRNS) 205
 - threat analysis 206–8

- future scope 216
- healthcare overview 186
 - healthcare evolution 186–7
 - healthcare information security 187
 - health security as a public health concept 188
 - need to implement privacy in healthcare data and information 187–8
- models for healthcare security 191
 - attribute role-based access control (ABAC) model 196
 - HIPAA privacy rules 203
 - HL7 role-based access control model 195–6
 - privacy access control model for e-healthcare service 196–7
 - RBAC healthcare model 192–4
 - security model for healthcare in big data 200–1
 - security model for healthcare in cloud computing 198–200
 - security model for healthcare in wireless sensor network 201–2
 - task role-based access control model 194–5
 - TMAC model 197–8
- privacy and security of EHR, recent development to maintain 174
 - advantages of blockchain over EHR 177
 - blockchain technology 176
 - comparison of cloud computing and blockchain 177
- privacy attacks 285
 - resistance against 288
- privacy concerns in healthcare information 34
 - major issues driving privacy front 34
 - real owner of patient data 34–5
 - role-based access and authorization 35–6
 - sharing data with external entities 35
 - social media penetration 35
- privacy laws and guidelines 36
 - Indian context 36–7
 - US context 37–8
- protecting patient data privacy 39
 - using blockchain for privacy protection 38
 - homomorphic encryption 38
 - state channels 39
- privacy impact assessment (PIA) 288
 - identifying the need for 289–90
 - integrating the PIA outcomes back into the project plan 298–9
 - signing off and recording the PIA outcomes 297–8
- privacy in EHR 9
 - access control model 10–11
 - grant access 10
 - issues 6–7
 - pseudonymity 10–11
- privacy management architecture 235–7
- privacy model in EMR 9
- privacy solutions, identify 294–7
- private key generator (PKG) 165
- privileges 76
- process authentication 66
- process-based identification 65–6
- process-centered HIS 313
- profiles of user 12–13, 50
- proof of stake 117
- Proof of Work (PoW) 117, 336
- protected health information (PHI) 36, 38, 52, 196
- protection and recover for health data 307
- protection framework and safety
 - standards related to EHRs 267
 - application implemented completely in the cloud 275–9
 - framework for the protection of personal information in the healthcare context 269

- implementation of a secure EHRs system in the cloud (case study) 272–3
- medical data processing by a professional 270–1
- from the optional computer to the cloud 273–5
- safety standards in EHRs 271–2
- security for healthcare communication 272
- special protection for sensitive data and prohibition of the processing of personal data 269–70
- provisioning 80
- proximity sensors 136–7
- p-sensitive k-anonymity property 239–41
- pseudonymity 10–11
- pseudonymization 237–9
- public and permissioned blockchains 116
- public key cryptography (PKC) 204, 209
 - accountability 211
 - attribute-based signatures (ABS) 211–12
 - attribute-based encryption (ABE) 209–10
 - ciphertext policy-based ABE (CP-ABE) 210
 - hybridized CP and KP-based ABE (CP-KEM-ABE) 211
 - key policy-based ABE (KP-ABE) 210–11
- public key encryption (PKE) 164–5
- public key infrastructure (PKI) 82, 123–4
- quality of service (QoS) 4
- quiet access to information 54
- Read Latency 317
- Read Throughput 317
- Redundant Byzantine Fault Tolerance Consensus Protocol (RBFT) 123
- redundant residual number systems (RRNS) 205
- regulatory framework, conflicting 190
 - authentication mechanisms 191
 - encryption technique 191
 - role-based access control model (RBAC) 191
- re-identification disclosure 241
- remote access 87–8
- remote access solutions 78
- repudiation 162
- requirements from electronic health system 96
 - increased patient control 97–8
 - interoperability and open systems 96–7
 - privacy and security 98–9
 - standardize structure of data, vocabulary, and nomenclature of these systems 96
- restrict information, rights to 55
- revolution in healthcare industries 3–4
- rights
 - providing 74–5
 - to restrict information 55
- ring signature 105
- role-based access and authorization 35–6
- role-based access control (RBAC) 10, 76, 82, 101, 191–4, 208, 230–1
- S&P issues, challenges in resolving 284–7
- safe EHR, implementation and design of 254–5
- safety and effectiveness of EHR 252–3
- safety imperfections in EHR 253
- safety measures for EHR systems 249
 - building a safety EHR safety metrics 262–3

- eHealth and teratology 262
- electronic healthcare report 251
 - EHR characteristics 251
 - EHR technical issues 251
 - mandatory safety for EHR in an organization 251–2
- medical data breach 256–7
- medical record maintenance 254
 - achieving performance in EHR 255
 - implementation and design of safe EHR 254–5
 - managing and preventing EHR-related flaws 255–6
- technical issues 257
 - customization of EHR 261–2
 - efficiency 261
 - emergency 262
 - organization of data 261–2
 - personalization 261
 - storing and preserving the storage of records for long pursuit 258–9
 - synchronization of records 259–61
- terminologies 252
 - EHR safety steps 253
 - safety and effectiveness of EHR 252–3
 - safety imperfections in EHR 253
 - using EHR as a tool in health care process 253–4
- traditional record maintenance in EHR 250–1
- safety standards in EHRs 271–2
- safety steps, EHR 253
- safety testing and reporting mechanism
 - achieving performance in EHR using 255
- SAN (Storage Area Network) 30
- scalability 161
- secret key (SK) 210
- secret key cryptography (SKC) 204
- Secure Socket Layer (SSL) 56
- security and privacy, challenges in 12
 - access control 12
 - data control 12
 - data security policies 12
 - integrity and confidentiality 12
 - misuse of health record 13
 - profiles of user 12–13
 - verification of user 12
- security and privacy issue in EHR 6–7, 113–14
- security and privacy issues in UK healthcare 283
 - challenges in resolving S&P issues 284
 - detailed problem analysis 284
 - enterprise, impact on 285
 - privacy attacks 285
 - security attacks 284–5
 - future directions 288
 - in healthcare infrastructure 283–4
 - proposed solution 285
 - overall solution description
 - resolving discussed S&P issues 285–7
 - privacy attacks, resistance against 288
 - security attacks, resistance against 287
 - scope and context 283
- security and privacy maintenance of EHR in existing technologies 163
 - attribute-based encryption (ABE) 165–6
 - attribute set based encryption 168–70
 - authentication schemes 171
 - biometric-based authentication 174
 - comparison of various authentication schemes 174
 - credential system 173
 - digital signature schemes 173
 - login/password with digital certificate 173

- password/PIN 173
- smart card based authentication schemes 173–4
- username/password 173
- comparison of various encryption techniques 171
- hierarchical attribute-based encryption 168
- hierarchical attribute set based encryption (HASBE) 170–1
- identity-based encryption (IBE) 165
- multiauthority attribute-based encryption 166–8
- public key encryption 164–5
- symmetric key encryption 163–4
- security and privacy model in EMR 9
- security architect 72–3
- security attacks 284–5
 - and goals 79–80
 - resistance against 287
- security concerns
 - curbing 33–4
 - in healthcare information 29
 - application security 29
 - audit trail 32
 - data availability 31–2
 - data breach and mandatory disclosure 32–3
 - data integrity 31
 - mock drills 32
 - periphery security 30
 - physical security 29
 - preserving confidentiality 31
 - server security 30
 - storage and communication security 30
 - ubiquitous device security 30
- security-critical system 228
- security for healthcare communication 272
- security goals (SG) 80
- security in EHR 11
- security issues in healthcare data and information 188
- data mining 190
- data ownership 189
- data storage 189
- data type 189
- regulatory framework, conflicting 190
 - authentication mechanisms 191
 - encryption technique 191
 - role-based access control model (RBAC) 191
- viewers of patient's medical records 190
- security monitoring 201
- security of a system 98
- security of EHR data 27–8
- security policies 12
- security principle 352–3
- security requirement (SR) for EHR 79, 160
 - availability 161
 - data integrity 160
 - data privacy 161
 - fine-grained access control 161
 - interoperability 160
 - scalability 161
 - user privacy 161
 - user revocation 161
- security standards 49
- sensitive data, special protection for 269–70
- sensitive personal data or information (SPI) 36
- sensitive personal information 36
- sensitive variables 241
- server security 30
- service denial 162
- session management 88
- sign-on controls 87
- simplicity (Si) 26
- Single Sign-On (SSO) facility 73, 78
- smart agriculture 143
- smart card based authentication schemes 173–4
- smart contract 375
- smart e-health gateway 84
- smoke/gas sensors 137

- Sovrin, working of 123–5
- spatial domain-based digital image
 - embedding 214
- Specialists/Physicians using the
 - EHRs 7
- spoofing attack 163
- state channels 39
- statistical disclosure control 229–30, 237
 - microaggregation 241–2
 - p-sensitive k-anonymity property 239–41
 - pseudonymization 237–9
- stenography 214–15
- storage and communication security 30
- storage and maintenance in health
 - data 307
- storage area network (SAN) 278
- StorageGRID 278–9
- storage of EHR data 27
- structure of EHR 95–6
- SwissGate* gateway 85
- symmetric key cryptography (SKC) 209
- symmetric key encryption 163–4
- synchronization of records 259–61
- systemic threats 227

- tag-based data model 233–5
- task role-based access control model 194–5
- TC 215 ISO/IEEE standards 312
- TC 215 ISO standards 312
- TC 215 ISO/TC standards 313
- TC 215 ISO/TR standards 313
- technical issues 251, 257
 - customization of EHR 261
 - efficiency 261
 - emergency 262
 - organization of data 261–2
 - personalization 261
- storing and preserving the storage of
 - records for long pursuit 258
 - NIST approach 258–9
- synchronization of records 259–61
- technological makeover 24
- technology, existing 158
 - cloud computing 158–60
 - fog computing 160
- temperature/humidity sensors 136
- test accounts, deletion of
 - after usage 79
- tethered PHRs 5
- threat analysis 206
 - information threats 207–8
 - intentional threats 207
 - natural threats 206–7
 - network threats 207
 - transmission threats 207
 - unintentional threats 207
- threats to access management 77
- threshold signatures 105
- TinySec 83
- TMAC model 197
 - C-TMAC model 198
 - T-TMAC model 198
- traditional clinical history (TCH) 267
- traditional medical care system,
 - workflow of 44–5
- traditional record maintenance in
 - EHR 250–1
- Transaction Latency 317
- transactions 230
- Transaction Throughput 317
- transmission threats 207
- T-TMAC model 198
- tyre pressure monitoring system (TPMS) 137

- ubiquitous device security 30
- UC Davis Health System (UCDHS) 307–11
- UK healthcare, security and privacy
 - issues in: *see* security and
 - privacy issues in UK healthcare
- unencrypted data storage 107
- unified threat management (UTM) 30
- unintentional threats 207
- usability, of EHR 25–6

- user account creation without any
 - approval 78–9
- username/password 173
- user privacy 161
- user profiles 12–13
- user registration 80
- user revocation 161
- users 75
- user verification 12, 49–50
- utilization of EHR system 8

- value-based systems 4
- verifiable claim 122–3
- verification of user 12, 49–50, 74
- “verifier” 65
- viewers of patient’s medical records 190

- water quality sensor 139
- Web Application Firewall (WAF) 30
- Wi-Fi (wireless fidelity) technology 134

- wireless body area network (WBAN) 215
- wireless sensor network (WSN),
 - security model for healthcare in 201–2
 - defending the threats and security procedures 202
 - authentication mechanism 202
 - encryption mechanism 202
- workflow
 - of electronic health record system 45–7
 - of traditional medical care system 44–5

- Zero Knowledge Proofs (ZKPs) 38
- Zigbee 134–5
- zk-SNARKs 38
- Z-wave 135

Security and Privacy of Electronic Healthcare Records

Concepts, paradigms and solutions

Hospitals, medical practices and healthcare organizations are implementing new technologies at breakneck speed. Yet privacy and security considerations are often an afterthought, putting healthcare organizations at risk of data security and privacy issues, fines, damage to their reputations, with serious potential consequences for the patients. Electronic Health Record systems (EHRs) consist of clinical notes, patient listings, lab results, imaging results and screening tests. EHRs are growing in complexity over time and requiring increasing amounts of data storage.

With the development of the IoT, the Cloud and Smart Cities frameworks, new privacy and security methods are being pursued to secure healthcare-based systems and platforms. Presenting a detailed framework as well as comparative case studies for security protection, data integrity, privacy preservation, scalability, and healthcare legislation, this edited volume covers state of the art research and addresses privacy and security methods and technologies for EHRs.

About the Editors

Sudeep Tanwar is an Associate Professor in the Computer Science and Engineering Department at the Institute of Technology of Nirma University, Ahmedabad, India. His research interests include Routings Issues in WSN, Blockchain Technology, computational aspects of Smart Grid, and Fog Computing.

Sudhanshu Tyagi is an Assistant Professor in the Department of Electronics and Communication Engineering at Thapar Institute of Engineering and Technology, Deemed University, Patiala, India. His research focuses on wireless sensor networks, 5G, and body area sensor networks.

Neeraj Kumar is Professor with the Department of Computer Science and Engineering at Thapar Institute of Engineering and Technology, Deemed University, Patiala, India. His research focuses on distributed systems, security and cryptography, and body area networks.

IET Book Series on e-Health Technologies

Series Editor: Professor Joel P. C. Rodrigues, the National Institute of Telecommunications (Inatel), Brazil and Instituto de Telecomunicações, Portugal

Demographic shifts in populations trigger opportunities for innovations in e-Health, m-Health, precision and personalized medicine, robotics, sensing, the Internet of Things, cloud computing, Big Data, Software Defined Networks, and network function virtualization. The integration of these technologies is however associated with many technological, ethical, legal, and social issues. This new Book Series aims to disseminate recent advances in the e-Health Technology field to help improve healthcare and wellbeing.

ISBN 978-1-78561-898-7



9 781785 618987 >



Healthcare Technologies

Security

Computing

The Institution of Engineering and Technology • www.theiet.org
978-1-78561-898-7