

ADVANCES IN CYBER SECURITY

CYBER SECURITY AND DIGITAL FORENSICS



Challenges and Future Trends



Edited By
Mangesh M. Ghonge
Sabyasachi Pramanik
Ramchandra Mangrulkar
Dac-Nhuong Le

 Scrivener
Publishing

WILEY

Cyber Security and Digital Forensics

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Advances in Cyber Security

Series Editors: Rashmi Agrawal and D. Ganesh Gopal

Scope: The purpose of this book series is to present books that are specifically designed to address the critical security challenges in today's computing world including cloud and mobile environments and to discuss mechanisms for defending against those attacks by using classical and modern approaches of cryptography, blockchain and other defense mechanisms. The book series presents some of the state-of-the-art research work in the field of blockchain, cryptography and security in computing and communications. It is a valuable source of knowledge for researchers, engineers, practitioners, graduates, and doctoral students who are working in the field of blockchain, cryptography, network security, and security and privacy issues in the Internet of Things (IoT). It will also be useful for faculty members of graduate schools and universities. The book series provides a comprehensive look at the various facets of cloud security: infrastructure, network, services, compliance and users. It will provide real-world case studies to articulate the real and perceived risks and challenges in deploying and managing services in a cloud infrastructure from a security perspective. The book series will serve as a platform for books dealing with security concerns of decentralized applications (DApps) and smart contracts that operate on an open blockchain. The book series will be a comprehensive and up-to-date reference on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations.

Publishers at Scrivener

Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Cyber Security and Digital Forensics

Edited by
Mangesh M. Ghonge
Sabyasachi Pramanik
Ramchandra Mangrulkar
and
Dac-Nhuong Le



WILEY

This edition first published 2022 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

© 2022 Scrivener Publishing LLC

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

Wiley Global Headquarters

111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials, or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-119-79563-6

Cover image: Pixabay.com

Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Preface	xvii
Acknowledgment	xxvii
1 A Comprehensive Study of Security Issues and Research Challenges in Different Layers of Service-Oriented IoT Architecture	1
<i>Ankur O. Bang, Udai Pratap Rao and Amit A. Bhusari</i>	
1.1 Introduction and Related Work	2
1.2 IoT: Evolution, Applications and Security Requirements	4
1.2.1 IoT and Its Evolution	5
1.2.2 Different Applications of IoT	5
1.2.3 Different Things in IoT	7
1.2.4 Security Requirements in IoT	8
1.3 Service-Oriented IoT Architecture and IoT Protocol Stack	10
1.3.1 Service-Oriented IoT Architecture	10
1.3.2 IoT Protocol Stack	11
1.3.2.1 Application Layer Protocols	12
1.3.2.2 Transport Layer Protocols	13
1.3.2.3 Network Layer Protocols	15
1.3.2.4 Link Layer and Physical Layer Protocols	16
1.4 Anatomy of Attacks on Service-Oriented IoT Architecture	24
1.4.1 Attacks on Software Service	24
1.4.1.1 Operating System-Level Attacks	24
1.4.1.2 Application-Level Attacks	25
1.4.1.3 Firmware-Level Attacks	25
1.4.2 Attacks on Devices	26
1.4.3 Attacks on Communication Protocols	26
1.4.3.1 Attacks on Application Layer Protocols	26
1.4.3.2 Attacks on Transport Layer Protocols	28
1.4.3.3 Attacks on Network Layer Protocols	28
1.4.3.4 Attacks on Link and Physical Layer Protocols	30

1.5	Major Security Issues in Service-Oriented IoT Architecture	31
1.5.1	Application – Interface Layer	32
1.5.2	Service Layer	33
1.5.3	Network Layer	33
1.5.4	Sensing Layer	34
1.6	Conclusion	35
	References	36
2	Quantum and Post-Quantum Cryptography	45
	<i>Om Pal, Manoj Jain, B.K. Murthy and Vinay Thakur</i>	
2.1	Introduction	46
2.2	Security of Modern Cryptographic Systems	46
2.2.1	Classical and Quantum Factoring of A Large Number	47
2.2.2	Classical and Quantum Search of An Item	49
2.3	Quantum Key Distribution	49
2.3.1	BB84 Protocol	50
	2.3.1.1 Proposed Key Verification Phase for BB84	51
2.3.2	E91 Protocol	51
2.3.3	Practical Challenges of Quantum Key Distribution	52
2.3.4	Multi-Party Quantum Key Agreement Protocol	53
2.4	Post-Quantum Digital Signature	53
2.4.1	Signatures Based on Lattice Techniques	54
2.4.2	Signatures Based on Multivariate Quadratic Techniques	55
2.4.3	Hash-Based Signature Techniques	55
2.5	Conclusion and Future Directions	55
	References	56
3	Artificial Neural Network Applications in Analysis of Forensic Science	59
	<i>K.R. Padma and K.R. Don</i>	
3.1	Introduction	60
3.2	Digital Forensic Analysis Knowledge	61
3.3	Answer Set Programming in Digital Investigations	61
3.4	Data Science Processing with Artificial Intelligence Models	63
3.5	Pattern Recognition Techniques	63
3.6	ANN Applications	65
3.7	Knowledge on Stages of Digital Forensic Analysis	65
3.8	Deep Learning and Modelling	67
3.9	Conclusion	68
	References	69

4	A Comprehensive Survey of Fully Homomorphic Encryption from Its Theory to Applications	73
	<i>Rashmi Salavi, Dr. M. M. Math and Dr. U. P. Kulkarni</i>	
4.1	Introduction	73
4.2	Homomorphic Encryption Techniques	76
4.2.1	Partial Homomorphic Encryption Schemes	77
4.2.2	Fully Homomorphic Encryption Schemes	78
4.3	Homomorphic Encryption Libraries	79
4.4	Computations on Encrypted Data	83
4.5	Applications of Homomorphic Encryption	85
4.6	Conclusion	86
	References	87
5	Understanding Robotics through Synthetic Psychology	91
	<i>Garima Saini and Dr. Shabnam</i>	
5.1	Introduction	91
5.2	Physical Capabilities of Robots	92
5.2.1	Artificial Intelligence and Neuro Linguistic Programming (NLP)	93
5.2.2	Social Skill Development and Activity Engagement	93
5.2.3	Autism Spectrum Disorders	93
5.2.4	Age-Related Cognitive Decline and Dementia	94
5.2.5	Improving Psychosocial Outcomes through Robotics	94
5.2.6	Clients with Disabilities and Robotics	94
5.2.7	Ethical Concerns and Robotics	95
5.3	Traditional Psychology, Neuroscience and Future Robotics	95
5.4	Synthetic Psychology and Robotics: A Vision of the Future	97
5.5	Synthetic Psychology: The Foresight	98
5.6	Synthetic Psychology and Mathematical Optimization	99
5.7	Synthetic Psychology and Medical Diagnosis	99
5.7.1	Virtual Assistance and Robotics	100
5.7.2	Drug Discovery and Robotics	100
5.8	Conclusion	101
	References	101
6	An Insight into Digital Forensics: History, Frameworks, Types and Tools	105
	<i>G Maria Jones and S Godfrey Winster</i>	
6.1	Overview	105
6.2	Digital Forensics	107
6.2.1	Why Do We Need Forensics Process?	107

6.2.2	Forensics Process Principles	108
6.3	Digital Forensics History	108
6.3.1	1985 to 1995	108
6.3.2	1995 to 2005	109
6.3.3	2005 to 2015	110
6.4	Evolutionary Cycle of Digital Forensics	111
6.4.1	Ad Hoc	111
6.4.2	Structured Phase	111
6.4.3	Enterprise Phase	112
6.5	Stages of Digital Forensics Process	112
6.5.1	Stage 1 - 1995 to 2003	112
6.5.2	Stage II - 2004 to 2007	113
6.5.3	Stage III - 2007 to 2014	114
6.6	Types of Digital Forensics	115
6.6.1	Cloud Forensics	116
6.6.2	Mobile Forensics	116
6.6.3	IoT Forensics	116
6.6.4	Computer Forensics	117
6.6.5	Network Forensics	117
6.6.6	Database Forensics	118
6.7	Evidence Collection and Analysis	118
6.8	Digital Forensics Tools	119
6.8.1	X-Ways Forensics	119
6.8.2	SANS Investigative Forensics Toolkit – SIFT	119
6.8.3	EnCase	119
6.8.4	The Sleuth Kit/Autopsy	122
6.8.5	Oxygen Forensic Suite	122
6.8.6	Xplico	122
6.8.7	Computer Online Forensic Evidence Extractor (COFEE)	122
6.8.8	Cellebrite UFED	122
6.8.9	OSForensics	123
6.8.10	Computer-Aided Investigative Environment (CAINE)	123
6.9	Summary	123
	References	123
7	Digital Forensics as a Service: Analysis for Forensic Knowledge	127
	<i>Soumi Banerjee, Anita Patil, Dipti Jadhav and Gautam Borkar</i>	
7.1	Introduction	127
7.2	Objective	128
7.3	Types of Digital Forensics	129
7.3.1	Network Forensics	129

7.3.2	Computer Forensics	142
7.3.3	Data Forensics	147
7.3.4	Mobile Forensics	149
7.3.5	Big Data Forensics	154
7.3.6	IoT Forensics	155
7.3.7	Cloud Forensics	157
7.4	Conclusion	161
	References	161
8	4S Framework: A Practical CPS Design Security Assessment & Benchmarking Framework	163
	<i>Neel A. Patel, Dhairya A. Parekh, Yash A. Shah and Ramchandra Mangrulkar</i>	
8.1	Introduction	164
8.2	Literature Review	166
8.3	Medical Cyber Physical System (MCPS)	170
8.3.1	Difference between CPS and MCPS	171
8.3.2	MCPS Concerns, Potential Threats, Security	171
8.4	CPSSEC vs. Cyber Security	172
8.5	Proposed Framework	173
8.5.1	4S Definitions	174
8.5.2	4S Framework-Based CPSSEC Assessment Process	175
8.5.3	4S Framework-Based CPSSEC Assessment Score Breakdown & Formula	181
8.6	Assessment of Hypothetical MCPS Using 4S Framework	187
8.6.1	System Description	187
8.6.2	Use Case Diagram for the Above CPS	188
8.6.3	Iteration 1 of 4S Assessment	189
8.6.4	Iteration 2 of 4S Assessment	195
8.7	Conclusion	200
8.8	Future Scope	201
	References	201
9	Ensuring Secure Data Sharing in IoT Domains Using Blockchain	205
	<i>Tawseef Ahmed Teli, Rameez Yousuf and Dawood Ashraf Khan</i>	
9.1	IoT and Blockchain	205
9.1.1	Public	208
9.1.1.1	Proof of Work (PoW)	209
9.1.1.2	Proof of Stake (PoS)	209
9.1.1.3	Delegated Proof of Stake (DPoS)	210
9.1.2	Private	210
9.1.3	Consortium or Federated	210

9.2	IoT Application Domains and Challenges in Data Sharing	211
9.3	Why Blockchain?	214
9.4	IoT Data Sharing Security Mechanism On Blockchain	216
9.4.1	Double-Chain Mode Based On Blockchain Technology	216
9.4.2	Blockchain Structure Based On Time Stamp	217
9.5	Conclusion	219
	References	219
10	A Review of Face Analysis Techniques for Conventional and Forensic Applications	223
	<i>Chethana H.T. and Trisiladevi C. Nagavi</i>	
10.1	Introduction	224
10.2	Face Recognition	225
10.2.1	Literature Review on Face Recognition	226
10.2.2	Challenges in Face Recognition	228
10.2.3	Applications of Face Recognition	229
10.3	Forensic Face Recognition	229
10.3.1	Literature Review on Face Recognition for Forensics	231
10.3.2	Challenges of Face Recognition in Forensics	233
10.3.3	Possible Datasets Used for Forensic Face Recognition	235
10.3.4	Fundamental Factors for Improving Forensics Science	235
10.3.5	Future Perspectives	237
10.4	Conclusion	238
	References	238
11	Roadmap of Digital Forensics Investigation Process with Discovery of Tools	241
	<i>Anita Patil, Soumi Banerjee, Dipti Jadhav and Gautam Borkar</i>	
11.1	Introduction	242
11.2	Phases of Digital Forensics Process	244
11.2.1	Phase I - Identification	244
11.2.2	Phase II - Acquisition and Collection	245
11.2.3	Phase III - Analysis and Examination	245
11.2.4	Phase IV - Reporting	245
11.3	Analysis of Challenges and Need of Digital Forensics	246
11.3.1	Digital Forensics Process has following Challenges	246
11.3.2	Needs of Digital Forensics Investigation	247
11.3.3	Other Common Attacks Used to Commit the Crime	248
11.4	Appropriateness of Forensics Tool	248
11.4.1	Level of Skill	248

11.4.2	Outputs	252
11.4.3	Region of Emphasis	252
11.4.4	Support for Additional Hardware	252
11.5	Phase-Wise Digital Forensics Techniques	253
11.5.1	Identification	253
11.5.2	Acquisition	254
11.5.3	Analysis	256
11.5.3.1	Data Carving	257
11.5.3.2	Different Curving Techniques	259
11.5.3.3	Volatile Data Forensic Toolkit Used to Collect and Analyze the Data from Device	260
11.5.4	Report Writing	265
11.6	Pros and Cons of Digital Forensics Investigation Process	266
11.6.1	Advantages of Digital Forensics	266
11.6.2	Disadvantages of Digital Forensics	266
11.7	Conclusion	267
	References	267
12	Utilizing Machine Learning and Deep Learning in Cybersecurity: An Innovative Approach	271
	<i>Dushyant Kaushik, Muskan Garg, Annu, Ankur Gupta and Sabyasachi Pramanik</i>	
12.1	Introduction	271
12.1.1	Protections of Cybersecurity	272
12.1.2	Machine Learning	274
12.1.3	Deep Learning	276
12.1.4	Machine Learning and Deep Learning: Similarities and Differences	278
12.2	Proposed Method	281
12.2.1	The Dataset Overview	282
12.2.2	Data Analysis and Model for Classification	283
12.3	Experimental Studies and Outcomes Analysis	283
12.3.1	Metrics on Performance Assessment	284
12.3.2	Result and Outcomes	285
12.3.2.1	Issue 1: Classify the Various Categories of Feedback Related to the Malevolent Code Provided	285
12.3.2.2	Issue 2: Recognition of the Various Categories of Feedback Related to the Malware Presented	286

12.3.2.3	Issue 3: According to the Malicious Code, Distinguishing Various Forms of Malware	287
12.3.2.4	Issue 4: Detection of Various Malware Styles Based on Different Responses	287
12.3.3	Discussion	288
12.4	Conclusions and Future Scope	289
	References	292
13	Applications of Machine Learning Techniques in the Realm of Cybersecurity	295
	<i>Koushal Kumar and Bhagwati Prasad Pande</i>	
13.1	Introduction	296
13.2	A Brief Literature Review	298
13.3	Machine Learning and Cybersecurity: Various Issues	300
13.3.1	Effectiveness of ML Technology in Cybersecurity Systems	300
13.3.2	Machine Learning Problems and Challenges in Cybersecurity	302
13.3.2.1	Lack of Appropriate Datasets	302
13.3.2.2	Reduction in False Positives and False Negatives	302
13.3.2.3	Adversarial Machine Learning	302
13.3.2.4	Lack of Feature Engineering Techniques	303
13.3.2.5	Context-Awareness in Cybersecurity	303
13.3.3	Is Machine Learning Enough to Stop Cybercrime?	304
13.4	ML Datasets and Algorithms Used in Cybersecurity	304
13.4.1	Study of Available ML-Driven Datasets Available for Cybersecurity	304
13.4.1.1	KDD Cup 1999 Dataset (DARPA1998)	305
13.4.1.2	NSL-KDD Dataset	305
13.4.1.3	ECML-PKDD 2007 Discovery Challenge Dataset	305
13.4.1.4	Malicious URLs Detection Dataset	306
13.4.1.5	ISOT (Information Security and Object Technology) Botnet Dataset	306
13.4.1.6	CTU-13 Dataset	306
13.4.1.7	MAWILab Anomaly Detection Dataset	307
13.4.1.8	ADFA-LD and ADFA-WD Datasets	307
13.4.2	Applications ML Algorithms in Cybersecurity Affairs	307

13.4.2.1	Clustering	309
13.4.2.2	Support Vector Machine (SVM)	309
13.4.2.3	Nearest Neighbor (NN)	309
13.4.2.4	Decision Tree	309
13.4.2.5	Dimensionality Reduction	310
13.5	Applications of Machine Learning in the Realm of Cybersecurity	310
13.5.1	Facebook Monitors and Identifies Cybersecurity Threats with ML	310
13.5.2	Microsoft Employs ML for Security	311
13.5.3	Applications of ML by Google	312
13.6	Conclusions	313
	References	313
14	Security Improvement Technique for Distributed Control System (DCS) and Supervisory Control-Data Acquisition (SCADA) Using Blockchain at Dark Web Platform	317
	<i>Anand Singh Rajawat, Romil Rawat and Kanishk Barhanpurkar</i>	
14.1	Introduction	318
14.2	Significance of Security Improvement in DCS and SCADA	322
14.3	Related Work	323
14.4	Proposed Methodology	324
14.4.1	Algorithms Used for Implementation	327
14.4.2	Components of a Blockchain	327
14.4.3	MERKLE Tree	328
14.4.4	The Technique of Stack and Work Proof	328
14.4.5	Smart Contracts	329
14.5	Result Analysis	329
14.6	Conclusion	330
	References	331
15	Recent Techniques for Exploitation and Protection of Common Malicious Inputs to Online Applications	335
	<i>Dr. Tun Myat Aung and Ni Ni Hla</i>	
15.1	Introduction	335
15.2	SQL Injection	336
15.2.1	Introduction	336
15.2.2	Exploitation Techniques	337
15.2.2.1	In-Band SQL Injection	337
15.2.2.2	Inferential SQL Injection	338
15.2.2.3	Out-of-Band SQL Injection	340

15.2.3	Causes of Vulnerability	340
15.2.4	Protection Techniques	341
15.2.4.1	Input Validation	341
15.2.4.2	Data Sanitization	341
15.2.4.3	Use of Prepared Statements	342
15.2.4.4	Limitation of Database Permission	343
15.2.4.5	Using Encryption	343
15.3	Cross Site Scripting	344
15.3.1	Introduction	344
15.3.2	Exploitation Techniques	344
15.3.2.1	Reflected Cross Site Scripting	345
15.3.2.2	Stored Cross Site Scripting	345
15.3.2.3	DOM-Based Cross Site Scripting	346
15.3.3	Causes of Vulnerability	346
15.3.4	Protection Techniques	347
15.3.4.1	Data Validation	347
15.3.4.2	Data Sanitization	347
15.3.4.3	Escaping on Output	347
15.3.4.4	Use of Content Security Policy	348
15.4	Cross Site Request Forgery	349
15.4.1	Introduction	349
15.4.2	Exploitation Techniques	349
15.4.2.1	HTTP Request with GET Method	349
15.4.2.2	HTTP Request with POST Method	350
15.4.3	Causes of Vulnerability	350
15.4.3.1	Session Cookie Handling Mechanism	350
15.4.3.2	HTML Tag	351
15.4.3.3	Browser's View Source Option	351
15.4.3.4	GET and POST Method	351
15.4.4	Protection Techniques	351
15.4.4.1	Checking HTTP Referer	351
15.4.4.2	Using Custom Header	352
15.4.4.3	Using Anti-CSRF Tokens	352
15.4.4.4	Using a Random Value for each Form Field	352
15.4.4.5	Limiting the Lifetime of Authentication Cookies	353
15.5	Command Injection	353
15.5.1	Introduction	353
15.5.2	Exploitation Techniques	354
15.5.3	Causes of Vulnerability	354

15.5.4	Protection Techniques	355
15.6	File Inclusion	355
15.6.1	Introduction	355
15.6.2	Exploitation Techniques	355
15.6.2.1	Remote File Inclusion	355
15.6.2.2	Local File Inclusion	356
15.6.3	Causes of Vulnerability	357
15.6.4	Protection Techniques	357
15.7	Conclusion	358
	References	358
16	Ransomware: Threats, Identification and Prevention	361
	<i>Sweta Thakur, Sangita Chaudhari and Bharti Joshi</i>	
16.1	Introduction	361
16.2	Types of Ransomwares	364
16.2.1	Locker Ransomware	364
16.2.1.1	Reveton Ransomware	365
16.2.1.2	Lcky Ransomware	366
16.2.1.3	CTB Locker Ransomware	366
16.2.1.4	TorrentLocker Ransomware	366
16.2.2	Crypto Ransomware	367
16.2.2.1	PC Cyborg Ransomware	367
16.2.2.2	OneHalf Ransomware	367
16.2.2.3	GPCode Ransomware	367
16.2.2.4	CryptoLocker Ransomware	368
16.2.2.5	CryptoDefense Ransomware	368
16.2.2.6	CryptoWall Ransomware	368
16.2.2.7	TeslaCrypt Ransomware	368
16.2.2.8	Cerber Ransomware	368
16.2.2.9	Jigsaw Ransomware	369
16.2.2.10	Bad Rabbit Ransomware	369
16.2.2.11	WannaCry Ransomware	369
16.2.2.12	Petya Ransomware	369
16.2.2.13	Gandcrab Ransomware	369
16.2.2.14	Rapid Ransomware	370
16.2.2.15	Ryuk Ransomware	370
16.2.2.16	Lockergoga Ransomware	370
16.2.2.17	PewCrypt Ransomware	370
16.2.2.18	Dhrama/Crysis Ransomware	370
16.2.2.19	Phobos Ransomware	371
16.2.2.20	Malito Ransomware	371

16.2.2.21	LockBit Ransomware	371
16.2.2.22	GoldenEye Ransomware	371
16.2.2.23	REvil or Sodinokibi Ransomware	371
16.2.2.24	Nemty Ransomware	371
16.2.2.25	Nephilim Ransomware	372
16.2.2.26	Maze Ransomware	372
16.2.2.27	Sekhmet Ransomware	372
16.2.3	MAC Ransomware	372
16.2.3.1	KeRanger Ransomware	373
16.2.3.2	Go Pher Ransomware	373
16.2.3.3	FBI Ransom Ransomware	373
16.2.3.4	File Coder	373
16.2.3.5	Patcher	373
16.2.3.6	ThiefQuest Ransomware	374
16.2.3.7	Keydnep Ransomware	374
16.2.3.8	Bird Miner Ransomware	374
16.3	Ransomware Life Cycle	374
16.4	Detection Strategies	376
16.4.1	UNEVIL	376
16.4.2	Detecting File Lockers	376
16.4.3	Detecting Screen Lockers	377
16.4.4	Connection-Monitor and Connection-Breaker Approach	377
16.4.5	Ransomware Detection by Mining API Call Usage	377
16.4.6	A New Static-Based Framework for Ransomware Detection	377
16.4.7	White List-Based Ransomware Real-Time Detection Prevention (WRDP)	378
16.5	Analysis of Ransomware	378
16.5.1	Static Analysis	379
16.5.2	Dynamic Analysis	379
16.6	Prevention Strategies	380
16.6.1	Access Control	380
16.6.2	Recovery After Infection	380
16.6.3	Trapping Attacker	380
16.7	Ransomware Traits Analysis	380
16.8	Research Directions	384
16.9	Conclusion	384
	References	384

Preface

Cyber security and digital forensics are an important topic nowadays, which provides many challenging issues in relation to security, identity, intrusion detection, advanced threat detection, privacy preservation etc.

The goal of this edited book is to outline the cyber security and digital forensic challenges and future trends. The book focuses on how to secure computers from hackers and how to deal with obtaining, storing, evaluating, analysing and presenting electronic evidences. Current threats are getting more complicated and advanced with the rapid evolution of adversarial techniques. Networked computing, and portable electronic devices have broadened the role of digital forensics beyond traditional investigations into computer crime.

The main focus of this book is to provide the reader with a broad coverage of the topics that includes different concepts, models, and terminology along with examples and illustrations to show substantial technical field details. It motivates readers to practice tougher security and defense processes to cope with attackers and mitigate the situation. Practically every crime now requires some aspect of digital evidence; digital forensics provides the techniques and instruments for articulating these evidences. Digital forensics also has a number of uses for information. In addition, it has a crucial role to play in information security, security breach investigations yield useful knowledge which can be used to develop more secure systems.

Increasing overall use of computers as a way to store and retrieve high-security information requires appropriate security measures to safeguard the entire computing and communication scenario. The facets of information security are becoming a primary concern with the introduction of social media and its technology to protect the networks and the cyber environment from various threats.

This book aims at young professionals of technology, privacy, and confidence to use and improve industry reliability in a distributed manner, as well as computer scientists and software developers seeking to conduct

research and develop cyber security and digital forensic tools. This book also benefits researchers and students of advanced computer science and information technology levels.

The book focuses on cutting-edge work from both academia and industry, and seeks to solicit original research chapters with specific emphasis on cyber security and digital forensic challenges and future trends. This book also outlines some of the exciting areas of future research in cyber security and digital forensics which will lead to additional innovations in this area of research.

Organization of the Book

The book is organized into 16 chapters. A brief description of each of the chapters follows:

Chapter 1

Service-Oriented Architecture (SOA) has proven its applicability on technologies like the Internet of Things (IoT). The major benefits of SOA architecture are flexibility, better information flow, re-usability and scalability, which make it worthy to use in IoT. This concept, when adopted with generic IoT architecture, creates layers that ask and deliver service to each other. Communication protocols play an important part here, but security always remains a major concern while dealing with a huge number of heterogeneous components of IoT. This chapter provides a survey of enabling protocols, the taxonomy of layer-wise attacks and security issues of the service-oriented IoT architecture. The chapter also describes major vulnerabilities related to the adaption of SOA into IoT. We feel that this chapter can give directions to researchers for enhancing security and privacy in IoT.

Chapter 2

Broadly, Cryptography refers to the passing of secret information from one place to another securely so that only intended receivers can decrypt it. Security of the modern public key cryptographic algorithms and protocols is mainly dependent on the complexity of the factorization of the product of large prime numbers. But due to technological developments in the field of computation and evolution of new mathematical techniques, the problem of the factorization of the product of integers is not complex anymore nowadays. The growing research interests in Quantum computing technology is also making the modern public cryptographic algorithms unsafe. Researchers have proved that modern cryptographic algorithms such as

RSA are breakable using quantum computers in polynomial time complexity. Therefore, attempts are being made to design new cryptographic algorithms using Quantum Computing techniques. Quantum cryptography is an emerging field which works on principles of quantum physics. In this paper, an attempt has been made to introduce quantum cryptography, analysis on supremacy of quantum cryptography over modern cryptography, discussion on key distribution using quantum physics, and implementation challenges in quantum key distribution. We have proposed two key verification mechanisms for BB84 protocol, analysis on quantum attacks on modern cryptographic digital signatures, post-quantum digital signatures and finally discussion on future directions of this technology.

Chapter 3

Constant growth in crime rates instigates computational resources for examination at a robust rate. Whatever data being examined with the help of forensic tools needs to be stored in the digital memory. Hence artificial intelligence is the upcoming machine learning technology which is comprehensive for human minds and provides capacity of digital storage media which can be accessed when in need. The purpose of our current research is to have broader understanding about the applicability of Artificial Intelligence (AI) along with computational logic tools analysis. The present artificial neural network helps in detection of criminals through comparison of faces by employing deep learning which offers neural networks. Thus, our paper focus on the computational forensic approaches built with AI applications to detect and predict possible future crimes. Several in-built algorithms control and create a model image in a camera which can be utilized in forensic casework to solve cases robustly.

Chapter 4

The adoption of cloud platforms is gradually increasing due to the several benefits of cloud computing. Despite the numerous benefits of cloud computing, data security and privacy is a major concern, due to lack of trust on cloud service provider (CSP). Data security can be achieved through the cryptographic techniques, but processing on encrypted data requires the sharing of a secret key with the CSP to perform operations on cloud data. This leads to the breach of data privacy. The power of cloud computing is fully utilized if one is able to perform computations on encrypted data outsourced to the cloud. Homomorphic Encryption (HE) enables to store data in encrypted form and perform computations on it without revealing the secret key to CSP. This chapter highlights existing HE techniques, their

implementations in various libraries, and existing work in the field of computations on homomorphic encryption used in various applications like healthcare, financial.

Chapter 5

This chapter is an attempt to theoretically analyze human behavior and the constructions of intelligent artifacts through robotics. It highlights how the process of human development and comprehension of human behavior can be marked as a flagpole in understanding the construction of robotic systems in the repertoire of motor, perceptual, and cognitive capabilities. Technologies such as artificial intelligence and Neuro Linguistic Programming (NLP) are helping in behavioral mapping. The various functions of talent on-boarding, talent development and the off-boarding process can help in effective management which can be utilized in people through synthetic psychology. This helps in rationally understanding human behavior through robotics. Further this gives an overview of human-robot interaction (HRI) and how they are helpful in mental health care, social skill development and improving the psychosocial outcome through robotics. Synthetic psychology's impact on neuroscience and its medical diagnostics are also discussed in the chapter. Implications, suggestions, and limitations along with the ethical issues are discussed for exploring the potential of this emerging technology.

Chapter 6

The world is increasingly interconnected with the internet, which acts as a nervous system for every organisation. We can easily find interconnected devices in every home in the form of Smart devices, computer networks, and so on. The data generated by mobile devices increases rapidly because of the increase in the huge number of mobile devices, which takes more time in analysing the digital evidence. The objective of this chapter is to contribute to the history of digital forensics, the Evolutionary cycle, various investigation phases of digital forensics and give a detailed explanation about the types involved in digital forensics. This chapter demonstrates a brief study about how digital evidence plays an important role in investigation. In addition to this, we also explained the forensics tools as commercial bases as well as open-source software. During the investigation phase, determining the appropriate forensics tools depends upon the digital devices and Operating System. In some cases, multiple tools can be used to extract the full digital data.

Chapter 7

Any machine exposed to the Internet today is at the risk of being attacked and compromised. The popularity of the internet is not only changing our life view, but also changing the view of crime in our society and all over the world. The reason for Forensic Investigation is increased computer crime. Digital technology is experiencing an explosion in growth and applications. This explosion has created the new concept of the cyber-criminal, and the need for security and forensics experts in the digital environment. The purpose of digital forensics is to answer investigative or legal questions to prove or disprove a court case. To ensure that innocent parties are not convicted and that guilty parties are convicted, it is mandatory to have a complete forensic process carried out by a qualified investigator who implements quality control measures and follows standards. In this paper, types of Digital Forensics with their tools and techniques of investigation are discussed. This chapter also involves the challenges in carrying out Digital forensics.

Chapter 8

A Cyber Physical System (CPS) is an amalgamation of multicomponent, networked intelligent digital systems with an ability to interact with humans in realtime and in usually uncertain physical environment. CPS finds its uses in multiple sectors including health care. The term ‘Medical Cyber Physical System’ (MCPS) describes a prominent branch of CPS pivoting its health care sector use cases. The use of MCPS increases the need to collect more data, process it, and to put it into action. With large amounts of data being collected, modelled, and trained to produce appropriate actions also sheds light towards CPS Security (CPSSEC) mechanisms. There exist multiple proposed security mechanisms for CPSs. However, there is a lack of consolidated framework to assess and benchmark its security aspects. In this chapter, authors have explained the need for such a framework for assessing the security of MCPSs and have proposed one, named 4S (Step-by-Step, Systematic, Score Based, Security Pivotal) Assessment and Benchmarking Framework. An assessment on a hypothetical MCPS has also been done to illustrate the use of the 4S framework. Such a framework can render useful for system designers and can also be improved by other researchers to strengthen the security aspect of MCPSs.

Chapter 9

Data in IoT domains is significantly analysed and the information is mined as required. The results from the devices are then shared among the interested devices for better experience and efficiency. Sharing of data

is rudimentary in any IoT platform which increases the probability of an adversary gaining access of the data. Blockchain, which consists of blocks that are connected together by means of cryptographic hashes, SHA256 being the most popularly used hash function in the blockchain network, is a newly adapted technology for secure sharing of data in IoT domains. A lot of challenges involving the integration for blockchain in IoT has to be addressed that would ultimately provide a secure mechanism for data sharing among IoT devices.

Chapter 10

Security systems have been one of the most challenging systems to secure assets and protect privacy over the past few years. Because of the increase in electronic transactions, the demand for rapid and precise identification and authentication is high. Face can be used as an identification and authentication tool. Face recognition possess many challenges like pose variation, blurriness, low resolution, illumination, facial expression, viewing angle and lighting conditions. Most of the work has been carried out to address the challenges in face recognition. Forensic face recognition is more challenging than normal face recognition because forensic images are of poor quality due to facial images captured under unfavorable circumstances. The forensic world is also becoming difficult and challenging because numerous crimes occur frequently and criminal investigators use face as a valuable and forensic tool. Forensic experts use domain-specific methods and perform a manual comparison to identify the suspects. The manual comparison takes more time and effort. As a result, it is possible to develop novel approaches to automate the process of domain-specific methods. The main objective of this chapter is to describe how face recognition is an important and most significant topic in forensics and the challenges which exist in forensic face recognition. From this chapter, researchers will be motivated to pursue research in the area of forensic face recognition since research in this field is at an infant stage.

Chapter 11

Traditional Computer Forensics seems to be no longer as trivial as decades ago, with a very restricted set of available electronic components, entering the age of digital formation of hardware and software too. It has recently been shown how cyber criminals are using a sophisticated and progressive approach to target digital and physical infrastructures, people and systems. Therefore, the analysis approach faces many problems due to the fact that billions of interconnected devices produce relatively at least small bits of evidence that comprehend the Data Analysis paradigm effortlessly. As a

consequence, the basic methodology of computer forensics requires to adapt major attention to develop smart and fast digital investigation techniques. Digital forensics investigation frameworks are occupied with lots of toolkits and applications according to the need of any criminal incident. Using the Digital Forensics Process's microscope, specific objects are discussed and analysed with respect to which tools are needful. Also, where the scope of attention is required to enhance the feature in it. This research leads to increased awareness, challenges and opportunities for Digital Forensics process with respect to different fields such as networks, IoT, Cloud computing, Database system, Big data, Mobile and handheld devices, Disk and different storage media, and Operating system.

Chapter 12

Machine learning (ML) and deep learning (DL) have both produced overwhelming interest and drawn unparalleled community interest recently. With a growing convergence of online activities and digital life, the way people have learned and function is evolving, but this also leads them towards significant security concerns. Protecting sensitive information, documents, networks and machine-connected devices from unwanted cyber threats is a difficult task. Robust cybersecurity protection is necessary for this reason. For a problem solution, current innovations like machine learning and deep learning is incorporated to cyber threats. This paper also highlights the problems and benefits with using ML/DL and presents recommendations for research directions for machine learning and deep learning in cybersecurity.

Chapter 13

Machine learning (ML) is the latest buzzword growing rapidly across the world, and ML possesses massive potential in numerous domains. ML technology is a subset of Artificial Intelligence (AI) and empowers digital machines with the ability to learn without being explicitly programmed, i.e., the capability to learn from past experiences. Since the last decade, ML technology has been used in various domains because it possesses numerous interesting characteristics such as adaptability, robustness, learnability, and its ability to take instant actions against unexpected challenges. The traditional cybersecurity systems are built on rules, attack signatures, and fixed algorithms. Thus, the systems can act only upon the '*knowledge*' fed to them and human intervention is continually required for the proper functioning of traditional cybersecurity systems. On the other hand, ML technology can recognize various patterns from past experiences and is capable of predicting or detecting future attacks based on seen or unseen

data. The ML technology is capable of handling massive real-time network data which allows various issues present in conventional cybersecurity systems to be overcome. In the present chapter, various issues related to the applications of ML in cybersecurity have been discussed. The effectiveness of applying ML technology in cybersecurity affairs has been thoroughly investigated. The contemporary challenges being faced by researchers in the realm have been identified and discussed. The current chapter presents available datasets and algorithms for the successful implementation of ML technology in the domain of cybersecurity. The datasets are also compared across various parameters. Finally, applications of ML practices by three renowned businesses, Facebook, Microsoft, and Google are explored.

Chapter 14

Blockchain will become the world's most basic technology—to go ahead. The revolution has actually already begun. The advent of distributed control system (DCS) and supervisory control and data acquisition (SCADA) has led to the necessity for automation, connection, and stable IoT Security systems from the dark web. There are no autonomous decision-making and real-time connectivity capabilities in existing innovative structures, a requirement for flexible, complex development systems. This research introduces to these tests an independent, stable, and interactive Blockchain-based framework. To connect computers, consumers, tools, dark web supplier, and other peers, it is possible to build with the Internet of Things (IoT) and cloud services in support of the proposed software. The recommendation would check the argument with a small, real-life IoT network blockchain using the Smart Contract functionality and reliable pair to open ledger functionality. A private Blockchain would operate on one board unit and bridge this case study to a micro-controller with IoT sensors. Distributed control system (DCS) and supervisory control and data acquisition (SCADA) in the dark web platform have been introduced to implement this device to study and analyze the existing approach with IoT-Towards Automated IoT Industry to improve the security system using blockchain technology.

Chapter 15

A developer must have an understanding ability of secure coding to create secure applications. A secure coding knowledge is focused on the combination of multiple mechanisms for exploiting and protecting typical malicious inputs to vulnerabilities of an application. The aim of this chapter is to review the recent techniques about exploitation and protection of common malicious inputs to online applications implemented by PHP script

for a developer to enhance the security of web pages. This chapter provides essential knowledge and mechanisms to vulnerabilities management for secure online applications.

Chapter 16

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Ransomware is a way of stealing money in which a user's files are encrypted and the decryption key is held by the attacker until a ransom amount is paid by the victim. Organizations need to have a full inventory of all the devices that are connected to the network and protect with an updated security solution. It is mandatory to study ransomware and its strategies to protect your computer system from being infected. Various types of ransomware attacks along with their features are studied by highlighting the major methodology used in the launching of ransomware attacks. Also, the comparative analysis of various ransoms, detection mechanisms as well as prevention policies against ransomware attacks are summarized.

Editors

Dr. Mangesh M. Ghonge

*Department of Computer Engineering, Sandip Institute of Technology
and Research Centre, Nashik, Maharashtra, India*

Dr. Sabyasachi Pramanik

*Department of Computer Science and Engineering, Haldia Institute
of Technology, Haldia, West Bengal, India*

Dr. Ramchandra Mangrulkar

*Department of Computer Engineering, D.J. Sanghvi College
of Engineering, Mumbai, Maharashtra, India*

Dr. Dac-Nhuong Le

*Associate Dean of Faculty of Information Technology,
Haiphong University, Vietnam*

Acknowledgment

We wish to acknowledge the help of all the people involved in this project and, more specifically, the authors and reviewers that took part in the review process. Without their support, this book would not have become a reality. We thank God for the opportunity to pursue this highly relevant subject at this time, and each of the authors for their collective contributions. Our sincere gratitude goes to all the chapter authors around the world who contributed their time and expertise to this book. We wish to acknowledge the valuable contributions of all the peer reviewers regarding their suggestions for improvement of quality, coherence, and content for chapters. Some authors served as referees; we highly appreciate their time and commitment. A successful book publication is the integrated result of more people than those persons granted credit as editor and author.

Editors

Dr. Mangesh M. Ghonge

*Department of Computer Engineering, Sandip Institute of Technology and
Research Centre, Nashik, Maharashtra, India*

Dr. Sabyasachi Pramanik

*Department of Computer Science and Engineering, Haldia Institute
of Technology, Haldia, India*

Dr. Ramchandra Mangrulkar

*Department of Computer Engineering, D.J. Sanghvi College
of Engineering, Mumbai, Maharashtra, India*

Dr. Dac-Nhuong Le

*Associate Dean of Faculty of Information Technology,
Haiphong University, Vietnam*

