
QUANTUM COMPUTING

in

CYBERSECURITY

Edited By

Romil Rawat, Rajesh Kumar Chakrawarti,
Sanjaya Kumar Sarangi, Jaideep Patel,
Vivek Bhardwaj, Anjali Rawat *and* Hitesh Rawat

 Scrivener
Publishing

WILEY

Quantum Computing in Cybersecurity

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

Publishers at Scrivener

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

Quantum Computing in Cybersecurity

Edited by
Romil Rawat
Rajesh Kumar Chakrawarti
Sanjaya Kumar Sarangi
Jaideep Patel
Vivek Bhardwaj
Anjali Rawat
and
Hitesh Rawat



WILEY

This edition first published 2023 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

© 2023 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 978-1-394-16633-6

Front cover images supplied by 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	xix
1 Cyber Quantum Computing (Security) Using Rectified Probabilistic Packet Mark for Big Data	1
<i>Anil V. Turukmane and Ganesh Khekare</i>	
1.1 Introduction	2
1.2 Denial-of-Service Attacks	3
1.2.1 DoS Attacks in Real Life	4
1.3 Related Work	5
1.3.1 Probabilistic Packet Marking (PPM)	6
1.3.1.1 DoS Attacks	6
1.3.1.2 FDPM	7
1.3.1.3 Simulation Surroundings via Extending ns2	7
1.4 Proposed Methodology	8
1.4.1 Denial of Service	8
1.4.1.1 Direct DDoS Attacks	9
1.4.1.2 Distributed DDoS Attacks	10
1.4.1.3 Reflector DDoS Attacks	10
1.5 Trace Back Mechanism for Rectified Probabilistic Packet Marking	10
1.5.1 A Brief Review of the Packet Marking Procedure	11
1.5.2 Packet Marking	12
1.5.3 Path Selection	12
1.5.4 Packet Sending	12
1.5.5 Packet Marking and Logging	12
1.5.6 Path Reconstruction	13
1.6 Conclusion	13
References	14

2	Secure Distinctive Data Transmission in Fog System Using Quantum Cryptography	17
	<i>Ambika N.</i>	
2.1	Introduction	18
2.2	Properties of Quantum Computing	19
2.3	Applications of Quantum Computing	22
2.4	Background	24
2.5	Literature Survey	25
2.6	Proposed Work	26
2.7	Analysis of the Study	27
2.8	Conclusion	29
	References	29
3	DDoS Attack and Defense Mechanism in a Server	33
	<i>Pranav Bhatnagar, Shreya Pai and Minhaj Khan</i>	
3.1	Introduction	34
3.2	DoS Attack	37
3.3	DDoS Attack	39
3.4	DDoS Mitigation	51
3.5	Conclusion	54
	Acknowledgement	55
	References	55
4	Dark Web Content Classification Using Quantum Encoding	57
	<i>Ashwini Dalvi, Soham Bhoir, Faruk Kazi and S. G. Bhirud</i>	
4.1	Introduction	58
4.2	Related Work	61
4.3	Proposed Approach	65
4.4	Result and Discussion	70
4.5	Conclusion	76
	References	77
5	Secure E-Voting Scheme Using Blockchain	81
	<i>Shrimoyee Banerjee and Umesh Bodkhe</i>	
5.1	Introduction	82
5.1.1	General Introduction	82
5.1.1.1	Key Components of the Blockchain Architecture	82
5.1.1.2	Characteristics of Blockchain Architecture	83
5.1.2	Electronic Voting System Using Quantum Blockchain	84
5.1.3	Architecture	85
5.1.4	Objective	86

5.1.5	Problem Statement	86
5.2	Literature Survey	87
5.2.1	Overview	87
5.3	Implementation and Methodology	89
5.3.1	Description	96
5.3.2	Installing Dependencies	99
5.3.3	Running	100
5.4	Result Analysis & Output	100
5.5	Conclusion and Future Directions	102
	References	102
6	An Overview of Quantum Computing–Based Hidden Markov Models	105
	<i>B. Abhishek, Sathian D., Amit Kumar Tyagi and Deepshikha Agarwal</i>	
6.1	Introduction	105
6.2	Elaboration of Hidden Quantum Markov Model	107
6.3	Example of HQMMs (Isolated Word Recognition in Action)	115
6.4	Matching of State Observation Density	117
6.5	Conclusion and Results	118
	References	119
7	Artificial Intelligence and Qubit-Based Operating Systems: Current Progress and Future Perspectives	121
	<i>Tejashwa Agarwal and Amit Kumar Tyagi</i>	
7.1	Introduction to OS, AI and ML	122
7.1.1	A Brief Summary	122
7.1.2	Different Components of AI Integrated with the OS	123
7.2	Learning Configurations	123
7.3	Building ML Models	124
7.4	Work Done in Improving Process Scheduling	124
7.4.1	OS Agents	125
7.5	Artificial Intelligence in Distributed Operating Systems	128
7.6	Current Progress	129
7.6.1	Advantages	132
7.6.2	Concerns	132
7.7	Quantum Artificial Intelligence	133
7.8	Conclusion	135
	References	135

8	Techno-Nationalism and Techno-Globalization: A Perspective from the National Security Act	137
	<i>Hepi Suthar, Hitesh Rawat, Gayathri M. and K. Chidambarathanu</i>	
8.1	Introduction	138
8.1.1	Techno-Globalism	138
8.1.2	National Security Act	141
8.1.2.1	Conditions when NSA can be Evoked	143
8.1.2.2	Safeguarding People Against the Act	144
8.1.2.3	Misuse of NSA	146
8.1.2.4	Need for Review	146
8.1.2.5	Critical Infrastructure and the Need of National Security Act's Reformation	147
8.1.3	Techno-Nationalism	148
8.1.3.1	Rise of Techno-Nationalism	150
8.1.3.2	The Rise of Industrial Policy Revolution	151
8.1.3.3	Human Capital as a Strategic Asset	152
8.1.3.4	Academic Institutions Being the New Ground Zero	152
8.1.3.5	Decoupling of the Knowledge Networks	152
8.1.3.6	Rise of China's Techno-Nationalism	153
8.1.3.7	China's Achievement so far in Collaboration with Taiwan	155
8.1.3.8	Techno-Nationalism: The Issue of Cyber Vulnerability won't be Resolved	158
8.2	Conclusion	161
	Acknowledgement	162
	References	162
9	Quantum Computing Based on Cybersecurity	165
	<i>P. William, Vivek Parganiha and D.B. Pardeshi</i>	
9.1	Introduction	166
9.2	Preliminaries	166
9.3	Threat Landscape	168
9.4	Defensive Measurements, Countermeasures, and Best Practises	170
9.5	Conclusion	171
	References	172
10	Quantum Cryptography for the Future Internet and the Security Analysis	175
	<i>P. William, A.B. Pawar and M.A. Jawale</i>	

10.1	Introduction	175
10.2	Related Works	177
10.3	Preliminaries	178
	10.3.1 Properties of Quantum Information	178
	10.3.2 Quantum Communication System	179
10.4	Quantum Cryptography for Future Internet	180
	10.4.1 Unconditional Security	180
	10.4.2 Sniffing Detection	182
	10.4.3 Security of the QKD	182
10.5	Conclusion	185
	References	186
11	Security Aspects of Quantum Cryptography	189
	<i>P. William, Siddhartha Choubey and Abha Choubey</i>	
11.1	Introduction	189
11.2	Literature Survey	190
11.3	Quantum Key Distribution	192
11.4	Cryptography	193
11.5	Quantum Cryptography with Faint Laser Pulses	195
11.6	Eavesdropping	196
11.7	Conclusion	198
	References	199
12	Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses	201
	<i>P. William, Vivek Parganiha and D.B. Pardeshi</i>	
12.1	Introduction	201
12.2	Quantum Computing Basics	202
	12.2.1 Qubits, Quantum Gates & Measurements	202
	12.2.2 Quantum Noise	203
	12.2.3 Quantum Neural Networks (QNN)	204
12.3	Security Applications	206
	12.3.1 PCB Defect Classification	206
	12.3.2 Hardware Trojan & Recycled Chip Detection	210
	12.3.3 Usage Model of QML in Hardware Security	210
12.4	Quantum Machine Learning	210
	12.4.1 Assets and Vulnerabilities	211
	12.4.2 Attack Models and Defenses Unreliable Hardware Allocator	212
12.5	Conclusion	213
	References	214

13 Cyber Forensics and Cybersecurity: Threat Analysis, Research Statement and Opportunities for the Future	217
<i>Nirav Bhatt and Amit Kumar Tyagi</i>	
13.1 Introduction	218
13.2 Background	219
13.3 Scope of this Work	220
13.4 Methodology and Analysis of Simulation Results	222
13.5 Quantum-Based Cybersecurity and Forensics	228
13.5.1 Quantum-Based Cybersecurity	228
13.5.2 Quantum-Based Forensics	229
13.6 Conclusion and Future Works	230
References	231
14 Quantum Computing: A Software Engineering Approach	233
<i>Mradul Agrawal, Aviral Jain, Rudraksh Thorat and Shivam Sharma</i>	
14.1 Introduction	234
14.2 Background of Research Area	235
14.3 Why Cryptography?	235
14.3.1 Application-to-Application Communication Reference	236
14.3.2 Modes of Block Cyphers	237
14.3.3 Secret Key Cryptography Algorithms in Use Today	238
14.4 Classical Cryptography	238
14.5 Quantum Cryptography (QCr)	239
14.6 Quantum Key Distribution	240
14.6.1 Application (Key-Related Work)	240
14.6.2 Problem Statement	242
14.7 Cryptanalysis	242
14.8 Entanglement	242
14.9 Quantum Teleportation	243
14.10 Applications of QCr in Cybersecurity	243
14.11 Quantum Key Distribution Protocols Implementation	244
14.12 Research and Work	244
14.13 Challenges Faced by QC	245
14.14 Limitations	245
14.15 Conclusion	246
References	246
15 Quantum Computing to the Advantage of Neural Network	249
<i>Aditya Maltare, Ishita Jain, Keshav Agrawal and Tanya Rawat</i>	
15.1 Introduction	250

15.2	Significance of Quantum Computers in Machine Learning	251
15.3	Related Work	252
15.4	Proposed Methodology	255
15.5	Result and Analysis	258
15.6	Conclusion	258
	Glossary	259
	References	260
16	Image Filtering Based on VQA with Quantum Security	263
	<i>Avni Burman, Bhushan Bawaskar, Harsh Dindorkar and Hrithik Surjan</i>	
16.1	Introduction	263
16.2	Related Work	267
16.3	Problem Statement	269
16.4	Working	269
16.5	Proposed Methodology Solution	270
16.6	Result Analysis	272
16.7	Conclusion	272
	References	273
17	Quantum Computing Techniques Assessment and Representation	275
	<i>Dewansh Khandelwal, Nimish Vyas, Priyanshi Skaktawat, Vaidehi Anwekar, Om Kumar C.U. and D. Jeyakumar</i>	
17.1	Introduction	276
	17.1.1 History of Computing	276
	17.1.2 Innovative Ways of Computing	276
	17.1.3 Need for QComp	277
17.2	Fundamentals of QC	278
17.3	Properties of QC	278
	17.3.1 Behaviour	278
	17.3.2 Superposition	279
	17.3.3 Entanglement	279
	17.3.4 Interference	279
17.4	Topography of QC	280
17.5	The Architecture of QC	281
	17.5.1 Hardware and Software of QCOMP	283
17.6	Quantum Algorithm	283
17.7	Design Limitations of Quantum Computer	284
17.8	Different Categories of Quantum Computer	286
	17.8.1 Analog Quantum Computer	286

17.8.2	NISQ Gate-Based Computer	286
17.8.3	Gate-Based Quantum Computer with Full Error Correction	286
17.9	Advantages of QC	287
17.10	Disadvantages of QC	287
17.11	Applications of QC	288
17.12	Major Challenges in QC	290
17.13	Conclusion	291
	References	292
18	Quantum Computing Technological Design Along with Its Dark Side	295
	<i>Divyam Pithawa, Sarthak Nahar, Vivek Bhardwaj, Romil Rawat, Ruchi Dronawat and Anjali Rawat</i>	
18.1	Introduction	296
18.2	Related Work	297
18.3	History and Evolution of QCOM	298
18.4	Components & Concepts that Make QCOM Possible	300
18.5	Plans for the Future Development of Quantum Computer	302
18.6	Dark Side of QCOM	306
18.7	Plans for Protection in Quantum Era	309
18.8	Conclusion	310
	References	310
19	Quantum Technology for Military Applications	313
	<i>Sarthak Nahar, Divyam Pithawa, Vivek Bhardwaj, Romil Rawat, Anjali Rawat and Kiran Pachlasiya</i>	
19.1	Introduction	314
19.2	Related Work	317
19.3	Overview of QTECH	318
19.3.1	Quantum Information Science	318
19.3.2	Qcomm	318
19.3.2.1	Quantum Simulations	319
19.3.2.2	Quantum Searching and Quantum Walks	319
19.3.2.3	Quantum Cryptanalysis	320
19.3.2.4	Quantum Linear Algebra	320
19.3.2.5	Quantum Optimisations	320
19.3.3	Quantum Communication and Cryptography	321
19.3.3.1	Post-Quantum Cryptography	321
19.3.3.2	Quantum Random Number Generator	321
19.3.3.3	Quantum Network	321

19.3.3.4	Quantum Key Distribution	322
19.3.4	Quantum Sensing and Metrology	322
19.3.4.1	Quantum Clocks	323
19.3.4.2	Quantum RF Antenna	323
19.3.4.3	Quantum Radar Technology	323
19.3.4.4	Quantum Electric, Magnetic and Inertial Forces Sensing	324
19.3.4.5	Quantum Imaging Systems	324
19.3.4.6	Other Sensors and Technology	325
19.4	QTECH in Defence	325
19.4.1	TRL and Time Horizon	325
19.4.2	QTech Countermeasures	326
19.4.3	Quantum Strategy	326
19.5	Military Applications of QTECH	327
19.5.1	Capabilities of Qcomm	327
19.5.2	Quantum Cybersecurity	327
19.5.3	Quantum PNT	327
19.5.4	Quantum Communication Network	328
19.5.5	Quantum Electronic Warfare	328
19.5.6	Quantum ISTAR	328
19.5.7	Chemical and Biological Simulations and Detection	329
19.5.8	New Material Design	329
19.5.9	Quantum Radar and Lidar	329
19.5.10	Quantum Space Warfare	330
19.5.11	Quantum Underwater Warfare	330
19.6	Challenges and Consequences of Quantum Warfare	331
19.6.1	Technical Repercussions and Difficulties	331
19.6.2	Challenges and Consequences for Ethics and Peace	332
19.6.3	Consequences and Challenges for Military	332
19.7	Conclusion	332
	References	333
20	Potential Threats and Ethical Risks of Quantum Computing	335
	<i>Apurva Namdev, Darshan Patni, Balwinder Kaur Dhaliwal, Sunil Parihar, Shrikant Telang and Anjali Rawat</i>	
20.1	Introduction	335
20.1.1	Knowledge of Quantum Computing	336
20.1.2	Limitations of Quantum Computing	336
20.1.3	Quantum Computer vs. Classical Computer	337
20.1.4	Diving Deep into Quantum Computers	338

20.1.5	Three Potential Ethical Issues Associated with Quantum Computing	338
20.1.6	Sensitive Data in the Open	338
20.2	Research Design & Methodology	339
20.2.1	Research Objectives	339
20.2.2	Primary Studies Selection	340
20.3	Brief In-Depth Overview of Possible Vulnerabilities	341
20.3.1	Quantum Technology's Risk to Cybersecurity	341
20.3.1.1	How may Cybersecurity be Improved by Using Quantum Computing?	341
20.3.1.2	Risks Associated with Quantum Computers	341
20.3.1.3	What is the Most Pressing Cybersecurity Issue that Executives are Presently Facing?	342
20.3.1.4	What Potential Risks Could Quantum Computing Pose?	343
20.3.1.5	Hacking Quantum Computers is Not Possible	343
20.3.1.6	Do Any Quantum Computers Exist Now that are Available for Purchase?	343
20.3.2	Ethical Conditions and Risks	344
20.3.3	Protect Yourselves Against these Threats	345
20.3.3.1	Implement Industry Security Guidelines	345
20.3.3.2	Establish Zero Trust	346
20.3.3.3	Automated Tools Deployment	346
20.3.3.4	Put Controlled Threat Detection into Practice	347
20.3.4	Potential Threats and Existing Risks	347
20.3.4.1	Cybersecurity	347
20.3.4.2	Access	348
20.3.4.3	Artificial Intelligence, Data Harvesting, and Privacy	348
20.3.4.4	Explainability	348
20.3.4.5	Global Tensions and the Quantum "Arms Race"	349
20.4	New Risks to be Created	349
20.4.1	Health Care and Life Sciences	349
20.4.2	Emerging Materials	349
20.5	Futuristic Picture of Quantum Ethics	350

20.5.1	Quantum Computing is Coming of Age	351
20.6	Conclusion	352
	References	352
21	Is Quantum Computing a Cybersecurity Threat?	353
	<i>Akshat Maheshwari, Manan Jain, Vindhya Tiwari, Mandakini Ingle and Ashish Chourey</i>	
21.1	Introduction	354
21.1.1	Need for Cybersecurity	355
21.1.2	What is Quantum Computing?	355
21.1.3	What is Cryptography?	356
21.1.4	Symmetric Cryptography	356
21.1.5	Asymmetric Cryptography	357
21.1.6	Classical and Quantum Cryptography	358
21.1.7	Quantum Computing's Effects on Existing Cryptography	359
21.1.8	Cryptography Does Not Mean Security	360
21.2	How QCom Threatens Cybersecurity	360
21.3	How QCom could Improve Cybersecurity	361
21.4	Quantum Cryptography and Its Applications	362
21.5	Proposed Methodology	363
21.5.1	The Threat of Quantum to Cybersecurity	363
21.5.2	QCom	364
21.5.3	QCom Challenge	365
21.6	Background/Objective	366
21.7	Conclusion	366
	References	367
22	Quantum Computing in Data Security: A Critical Assessment	369
	<i>Sadullah Khan, Chintan Jain, Sudhir Rathi, Prakash Kumar Maravi, Arun Jhapate and Divyani Joshi</i>	
22.1	Introduction	370
22.2	Present Cryptographic Algorithms and Systems	371
22.3	Comparing Traditional Computing and Quantum Computing	373
22.4	Post-Quantum Cryptography (PQC)	377
22.5	Quantum Cryptography and Its Applications	378
22.6	Corporate Competitions Towards Quantum Computing	383
22.7	Threats Posed to Critical Infrastructure and Mechanisms	384
22.8	Conclusion	388
	References	389

23 Quantum Computing and Security Aspects of Attention-Based Visual Question Answering with Long Short-Term Memory	395
<i>Madhav Shrivastava, Rajat Patil, Vivek Bhardwaj, Romil Rawat, Shrikant Telang and Anjali Rawat</i>	
23.1 Introduction	396
23.1.1 Visual Question Answering	399
23.2 Literature Review	399
23.2.1 Attention within Sequences	400
23.2.2 Quantum Backdoor Attack Study	400
23.3 Problem Statement	401
23.4 Problem Elaboration	401
23.5 Proposed Methodology	402
23.6 Methods	404
23.6.1 Threat Model	404
23.6.2 Backdoor Design	404
23.6.3 The Optimized Patches and Recovery	405
23.6.4 Metrics Measures	406
23.7 Solution Approach	407
23.8 Expected Results	407
23.8.1 Explainable Recommendations System	407
23.8.2 VQA System	408
23.8.3 Quantum Security Aspect	408
23.9 Conclusion	409
23.10 Abbreviations	410
References	411
24 Quantum Cryptography – A Security Architecture	413
<i>Sunandani Sharma, Sneha Agrawal, Sneha Baldeva, Diya Dabhade, Parikshit Bais and Ankita Singh</i>	
24.1 Introduction	413
24.1.1 Organisation	414
24.2 Related Work	414
24.3 Properties of Quantum Information	415
24.4 Methodology	416
24.5 Supported Explanation	418
24.6 Conclusion	422
References	422
25 Quantum Computing Anomalies in Communication	425
<i>Anushka Ayachit, Jahanvee Sharma, Bhupendra Panchal, Sunil Patil, Safdar Sardar Khan and Rijvan Beg</i>	
25.1 Introduction	425
25.2 Significance of Quantum Computing	427

25.2.1	Working of Quantum Computers	432
25.3	The Dark Side of Quantum Computing	433
25.4	Previous Works	436
25.5	Conclusion	437
	References	438
26	Intrusion Detection System via Classical SVM and Quantum SVM: A Comparative Overview	441
	<i>Ananya Upadhyay, Ruchir Namjoshi, Riya Jain, Jaideep Patel and Gayathri M.</i>	
26.1	Introduction	442
26.2	Related Work	443
26.3	Models for IDS	443
26.3.1	Classical Support Vector Machine Model	444
26.3.1.1	Classical Support Vector in IDS	445
26.3.1.2	Limitations of Classical SVM	446
26.3.2	Quantum SVM Model	446
26.3.2.1	Quantum Support Vector in IDS	448
26.4	Conclusion	449
	References	449
27	Quantum Computing in Military Applications and Operations	453
	<i>Aman Khubani, Anadi Sharma, Axith Choudhary, Om Shankar Bhatnagar and K. Chidambarathanu</i>	
27.1	Introduction	454
27.2	Literary Survey	455
27.3	Definition	456
27.3.1	Introduction	456
27.3.2	A Key Quantum Principle	457
27.3.2.1	Qubit	457
27.3.2.2	Qsup	457
27.3.2.3	Qent	458
27.3.2.4	Photon Polarization	459
27.3.2.5	Heisenberg's Uncertainty Principle	459
27.3.2.6	Quantum Teleportation	460
27.3.3	QC	461
27.3.4	Quantum Internet	461
27.3.5	Quantum Sensing	461
27.4	Quantum Military Applications	462
27.5	Applications of QCRYP	465
27.6	Limitations	468
27.7	Conclusion	468
	References	468

28 Quantum Cryptography Techniques: Evaluation	471
<i>Shashank Sharma, T.M.Thiyagu, Om Kumar C.U. and D. Jeyakumar</i>	
28.1 Introduction	472
28.2 Quantum Technology (QTech) in Defence	473
28.2.1 Quantum Strategy	474
28.2.2 QTech Military Applications	475
28.3 The QKD Model	476
28.4 Related Work	478
28.5 Preliminaries	479
28.5.1 Quantum Information Properties	479
28.5.2 Quantum Communication System	480
28.6 QKD Protocols Implementation	482
28.6.1 Sifting	482
28.6.2 Error Correction	483
28.6.3 Privacy Amplifications	483
28.6.4 Authentication	483
28.7 Risk Analysis	483
28.8 Applications of Quantum Cryptography	484
28.9 Challenges of Quantum Cryptography	485
28.10 Conclusion and Future Work	486
References	486
29 Cyber Crime Attack Vulnerability Review for Quantum Computing	489
<i>Vaishnavi Gawde, Vanshika Goswami, Balwinder Kaur Dhaliwal, Sunil Parihar, Rupali Chaure and Mandakini Ingle</i>	
29.1 Introduction	490
29.1.1 Uses of QC	491
29.2 Significance of Cyber Crime Attack for QC	492
29.3 Related Work	493
29.4 Proposed Methodology	494
29.4.1 Threats Posed to Critical Infrastructure and Mechanisms	498
29.5 Conclusion	500
References	501
About the Editors	505
Index	507

Preface

The main topics of this book are:

- Quantum Inspired Community Classification in Social Networks Analytics
- Future Directions in Quantum Computing
- Quantum Machine Learning for Intrusion Detection
- Quantum Designs to Detect Distributed Denial of Service Attacks
- Cyber Terrorism for Quantum Internet
- Cryptography, and
- Cyber Criminals' Quantum Communication Networks

The security and effectiveness of communications in network infrastructures might be improved by quantum technology in a previously unheard-of way. This book, written as a complete and thorough text, guides readers through mathematically challenging topics in a way that encourages student participation.

In the context of criminality and forensics, this book offers a clear, step-by-step explanation of quantum computing. A deeper comprehension of the human and social dimensions of pertinent complexities, such as child sexual exploitation, violent radicalization, trafficking, disinformation and fake news, corruption, and cyber criminality, as well as victim support, must serve as the foundation for improved cyber-crime prevention, investigation, and remediation. Applications and solutions based on quantum computing that analyse massive volumes of data in near-real time in order to stop criminal activities or combat false information and disinformation while addressing security issues. In order to confront crime, including cybercrime and terrorism as well as various types of serious and organized crime, this will help security agencies incorporate such details into the operating processes of police officials (such as smuggling, money laundering, identity theft, counterfeiting of products, trafficking of illicit drugs and

falsified or substandard medicines, environmental crime, or illicit trafficking of cultural goods).

Cybercriminals employ cutting-edge tools, such as machine learning methods, to build and spread deadly malware using vast amounts of data. Cyber attackers can develop a ground-breaking means of evading cyber security by using quantum computing, which would enable them to quickly assess vast datasets before launching a sophisticated attack on several networks and devices.

Cyber Quantum Computing (Security) Using Rectified Probabilistic Packet Mark for Big Data

Anil V. Turukmane* and Ganesh Khekare

*Department of Computer Science Engineering, Parul University, Vadodar,
Gujarat, India*

Abstract

In recent years, denial-of-service (DoS) assaults have been a system flaw. DoS disobedience testing has become one of the most important streams in system Quantum Computing Security). This dynamic field of investigation has yielded astounding frameworks such as pushback message, ICMP take after back, and following package improvement methods. In tributary regarded informatics, the probabilistic packet marking (PPM) standard drew in considerable thinking. To begin with, the alluring purpose of this informatics follow-up approach is that it permits alterations to etch bound data on ambush packages that support chosen likelihood. After gathering a sufficient number of examined packages, the loss (or information plan centre) will construct a set of systems that offence groups crossed and, as a result, the setback will be assigned zones. The goal of the PPM algorithmic project is to demonstrate that produced outline is the same as offence graph, where relate degree attack outline is that course of action of techniques ambush packs investigated and created outline could be diagrammed by PPM algorithmic framework. The main goal of the structure is to provide a powerful approach to cope with tracking down an assailant's back IP address through a media like the internet. The system will stamp every shipment that is to be traded over the internet as indicated by the group's substance and deliver it via trade media. When it reaches its final destination, the stamping of any package is altered, and the structure is ready to be taken. The majority of PPM concerns have entailed a few issues such as loss of stamping information, issues recreating ambush routes, and low precision than on. In the first paper, we propose a dynamic probabilistic packet

*Corresponding author: anil.turukmane21100@paruluniversity.ac.in

marking (DPPM) approach as a replacement for another upgrade reasonability of PPM. On the other hand, if you're utilising mounted checking likelihood, we propose gauging regardless of whether the package has been stamped or not, and then selecting the appropriate checking likelihood. Most of the problems with the PPM approach could be solved using DPPM. A formal examination reveals that DPPM outperforms PPM in a variety of ways. The proposed solution is useful in domains where it is important to keep track of back IP addresses while changing the package, such as cybercrime and the illegal treatment of data groups where certain basic information must be transferred. Propose a P Packet M basic end condition, which is commonly omitted or not explicitly stated in writing. Due to the new end condition, the client of a new control has more freedom to inspect the precision of the chart that has been created.

Keywords: Quantum Computing (Security), Quantum Cryptography and Quantum Computing (Security), control mechanism, cyber crime, quantum attacks

1.1 Introduction

Over the last two decades, the world has seen significant advances in science and innovation that have successfully met a wide spectrum of human needs. These requests range from basic necessities like power bills and rail ticket reservations to more complex ones like force matrices for the era of violence and sharing. These advancements have raised the standard of human existence in terms of modernity and simplicity. Unexpectedly, a competing invention for negotiating Quantum Computing (Security) has evolved, with its own set of repercussions, hindering innovation. Robbery, hacking, and the blackout of private information are examples of information-related attacks. Anonymous subterranean attack networks that can efficiently assault a specific target every time are likely to be available, according to the media and many types of network Quantum Computing (Security) literature. This merely depicts a possible transition from today's attack to future attacks. Everything is on the table in the present world, from "damage and devastation" wars to "information warfare," to the negotiation of the aforementioned attack. Finally, attackers/networks that can hide are usually the ones who carry out these attacks.

The scope of attacks on targets is as extensive as that of constructional technology, but this thesis focuses on a specific sort of attack known as denial-of-service (DoS) attacks. DoS assaults are a form of targeted attack whose purpose is to deplete the target's resources and, as a result, prohibit large customers from obtaining service. For quite some time, great focus has been placed on the Quantum Computing (Security) of network

infrastructure, which has continued to be used for a variety of transactions. The internet Quantum Computing (Security) business, academia, and even the United States Conference, which has organized multiple conferences on the subject, have all taken notice [1, 2]. Various safety strategies have been proposed, each attempting to address a different set of issues. The anonymous attack is the specific risk that this research focuses on. Because the Source Address (SA) information is spoofed in the attack packages, the identity of the attacker(s) is not immediately visible to the individual in anonymous attacks.

1.2 Denial-of-Service Attacks

The focus of this thesis is on service denial (DoS) attacks on PC networks. The goal of these attacks is to deny legitimate users access to network services. This PhD includes a comprehensive look at many attack and defence mechanisms, as well as unique defensive mechanisms and new information on defensive mechanism selection and evaluation. DoS mitigation is an important part of network and computer Quantum Computing (Security). Network and computer Quantum Computing (Security) are frequently discussed in scientific domains. Computer Quantum Computing (Security) language is still imbalanced, which is a big issue [10, 11]. Computer and network Quantum Computing (Security) were originally prioritised in the mid-1970s, and some of the most meticulous Quantum Computing (Security) documentation was published in [12]. Denial-of-service attacks come in a variety of forms, and the number of them is expanding all the time as new procedures and data networks are developed. These attacks should be divided into two categories: physical and virtual, with the purpose of better comprehending the most common denial-of-service (DoS) attempts (or network-based). There are two other types of attacks that fall within this category, each of which represents the attack's overall goal: disabling critical services and draining system resources [13].

An Overview of Denial-of-Service Attacks

System disruption (DoS) attacks have been shown to be a significant and long-term threat to users, businesses, and internet infrastructure [16–20]. Blocking access to a specific object, such as a web application, is one of the key targets of these assaults. There have been numerous DoS guards proposed in the literature, but none of them can be trusted with any degree of certainty. Vulnerable hosts on the internet, as well as attack traffic sources,

are virtually certain to be exploited. It's just not possible to keep every host on the internet secure at all times. (In July 2005 it was assessed that there were roughly 350,000 hosts on the internet.) Furthermore, detecting and channelling legitimate traffic attacks without causing legal traffic injury to collateral is quite difficult.

A DoS attack can be carried out in one of two ways: as a flood or as a logical attack. A flood DoS attack is based on brute force. A victim is given as much information as possible, even if it is unneeded. This squandering of network bandwidth fills space with unnecessary data (e.g., spam mail, garbage files, and deliberate error messages), loads flawed data onto fixed-size data structures inside host software, and necessitates a significant amount of data management effort. To increase the impact of DoS attacks, they might continue to be planned from multiple sources (Distributed DoS, DDoS).

1.2.1 DoS Attacks in Real Life

Actual internet DoS instances were investigated throughout the popular era of 1989 to 1995. The three most common consequences were as follows: in 51% of the cases, there was a circle, and in 33% of the cases, there was a network decline of 33%, and in 26% of the cases, certain vital data was deleted. A single occasion can result in a variety of problems (the whole of rates is more than 100%). A college was the target of the first big DDoS attack in August 1999. This attack disabled the target's network for two days. On February 7, 2000, a few key web-based locations were attacked, and they were cut off from the internet for many hours. These DDoS attacks may occasionally cause a single victim's assault movement of around 1 Gbit/s.

The quantity, duration, and location of distributed denial-of-service (DDoS) attacks on the internet were tracked using scatter monitoring. Backscatter is defined as the victim's spontaneous reflex movement in response to the assault package, which is sent with fake IP addresses. In the three weeks of investigation in February 2001, over 12,000 attacks were registered against over 5,000 distinct victims. Packet fragmentation was studied in real networks. Bugs in fragmented management software are exploited in various logic DoS assaults, and the results of this emphasis still suggest the presence of such DoS on the web.

According to the Associated Press, the Emergency Response Team (CERT) Operations Unit was attacked in May 2001. Its portal was down for a few days due to a distributed denial of service (DDoS) attack. In the mid-2002, ISPs in the United Kingdom were focusing on DDoS assaults. Some

Also of Interest

From the same editors

ROBOTIC PROCESS AUTOMATION, Edited by Romil Rawat, Rajesh Kumar Chakrawarti, Sanjaya Kumar Sarangi, Rahul Choudhary, Anand Singh Gadwal, and Vivek Bhardwaj, ISBN: 9781394166183. Presenting the latest technologies and practices in this ever-changing field, this groundbreaking new volume covers the theoretical challenges and practical solutions for using robotics across a variety of industries, encompassing many disciplines, including mathematics, computer science, electrical engineering, information technology, mechatronics, electronics, bioengineering, and command and software engineering.

AUTONOMOUS VEHICLES VOLUME 1: Using Machine Intelligence, Edited by Romil Rawat, A. Mary Sowjanya, Syed Imran Patel, Varshali Jaiswal, Imran Khan, and Allam Balaram. ISBN: 9781119871958. Addressing the current challenges, approaches and applications relating to autonomous vehicles, this groundbreaking new volume presents the research and techniques in this growing area, using Internet of Things, Machine Learning, Deep Learning, and Artificial Intelligence.

AUTONOMOUS VEHICLES VOLUME 2: Smart Vehicles for Communication, Edited by Romil Rawat, Purvee Bhardwaj, Upinder Kaur, Shrikant Telang, Mukesh Chouhan, and K. Sakthidasan Sankaran, ISBN: 9781394152254. The companion to *Autonomous Vehicles Volume 1: Using Machine Intelligence*, this second volume in the two-volume set covers intelligent techniques utilized for designing, controlling and managing vehicular systems based on advanced algorithms of computing like machine learning, artificial Intelligence, data analytics, and Internet of Things with prediction approaches to avoid accidental damages, security threats, and theft.

Check out these other related titles from Scrivener Publishing

FACTORIES OF THE FUTURE: Technological Advances in the Manufacturing Industry, Edited by Chandan Deep Singh and Harleen Kaur, ISBN: 9781119864943. The book provides insight into various technologies adopted and to be adopted in the future by industries and measures the impact of these technologies on manufacturing performance and their sustainability.

AI AND IOT-BASED INTELLIGENT AUTOMATION IN ROBOTICS, Edited by Ashutosh Kumar Dubey, Abhishek Kumar, S. Rakesh Kumar, N. Gayathri, Prasenjit Das, ISBN: 9781119711209. The 24 chapters in this book provide a deep overview of robotics and the application of AI and IoT in robotics across several industries such as healthcare, defense, education, etc.

SMART GRIDS FOR SMART CITIES VOLUME 1, Edited by O.V. Gnana Swathika, K. Karthikeyan, and Sanjeevikumar Padmanaban, ISBN: 9781119872078. Written and edited by a team of experts in the field, this first volume in a two-volume set focuses on an interdisciplinary perspective on the financial, environmental, and other benefits of smart grid technologies and solutions for smart cities.

SMART GRIDS FOR SMART CITIES VOLUME 2: Real-Time Applications in Smart Cities, Edited by O.V. Gnana Swathika, K. Karthikeyan, and Sanjeevikumar Padmanaban, ISBN: 9781394215874. Written and edited by a team of experts in the field, this second volume in a two-volume set focuses on an interdisciplinary perspective on the financial, environmental, and other benefits of smart grid technologies and solutions for smart cities.

SMART GRIDS AND INTERNET OF THINGS, Edited by Sanjeevikumar Padmanaban, Jens Bo Holm-Nielsen, Rajesh Kumar Dhanaraj, Malathy Sathyamoorthy, and Balamurugan Balusamy, ISBN: 9781119812449. Written and edited by a team of international professionals, this groundbreaking new volume covers the latest technologies in automation, tracking, energy distribution and consumption of Internet of Things (IoT) devices with smart grids.

DESIGN AND DEVELOPMENT OF EFFICIENT ENERGY SYSTEMS, edited by Suman Lata Tripathi, Dushyant Kumar Singh, Sanjeevikumar Padmanaban, and P. Raja, ISBN 9781119761631. Covering the concepts and fundamentals of efficient energy systems, this volume, written and edited by a global team of experts, also goes into the practical applications that can be utilized across multiple industries, for both the engineer and the student.

INTELLIGENT RENEWABLE ENERGY SYSTEMS: Integrating Artificial Intelligence Techniques and Optimization Algorithms, edited by Neeraj Priyadarshi, Akash Kumar Bhoi, Sanjeevikumar Padmanaban, S. Balamurugan, and Jens Bo Holm-Nielsen, ISBN 9781119786276. This collection of papers on artificial intelligence and other methods for improving renewable energy systems, written by industry experts, is a reflection of the state of the art, a must-have for engineers, maintenance personnel, students, and anyone else wanting to stay abreast with current energy systems concepts and technology.

SMART CHARGING SOLUTIONS FOR HYBRID AND ELECTRIC VEHICLES, edited by Sulabh Sachan, Sanjeevikumar Padmanaban, and Sanchari Deb, ISBN 9781119768951. Written and edited by a team of experts in the field, this is the most comprehensive and up to date study of smart charging solutions for hybrid and electric vehicles for engineers, scientists, students, and other professionals.