
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

Table of Contents

[Cover](#)

[Table of Contents](#)

[Series Page](#)

[Title Page](#)

[Copyright Page](#)

[Preface](#)

[1 Cyber Quantum Computing \(Security\) Using Rectified Probabilistic Packet Mark for Big Data](#)

[1.1 Introduction](#)

[1.2 Denial-of-Service Attacks](#)

[1.3 Related Work](#)

[1.4 Proposed Methodology](#)

[1.5 Trace Back Mechanism for Rectified Probabilistic Packet Marking](#)

[1.6 Conclusion](#)

[References](#)

[2 Secure Distinctive Data Transmission in Fog System Using Quantum Cryptography](#)

[2.1 Introduction](#)

[2.2 Properties of Quantum Computing](#)

[2.3 Applications of Quantum Computing](#)

[2.4 Background](#)

[2.5 Literature Survey](#)

[2.6 Proposed Work](#)

[2.7 Analysis of the Study](#)

[2.8 Conclusion](#)

References

3 DDoS Attack and Defense Mechanism in a Server

3.1 Introduction

3.2 DoS Attack

3.3 DDoS Attack

3.4 DDoS Mitigation

3.5 Conclusion

Acknowledgement

References

4 Dark Web Content Classification Using Quantum Encoding

4.1 Introduction

4.2 Related Work

4.3 Proposed Approach

4.4 Result and Discussion

4.5 Conclusion

References

5 Secure E-Voting Scheme Using Blockchain

5.1 Introduction

5.2 Literature Survey

5.3 Implementation and Methodology

5.4 Result Analysis & Output

5.5 Conclusion and Future Directions

References

6 An Overview of Quantum Computing-Based Hidden Markov Models

6.1 Introduction

6.2 Elaboration of Hidden Quantum Markov Model

[6.3 Example of HQMMs \(Isolated Word Recognition in Action\)](#)

[6.4 Matching of State Observation Density](#)

[6.5 Conclusion and Results](#)

[References](#)

[7 Artificial Intelligence and Qubit-Based Operating Systems: Current Progress and Future Perspectives](#)

[7.1 Introduction to OS, AI and ML](#)

[7.2 Learning Configurations](#)

[7.3 Building ML Models](#)

[7.4 Work Done in Improving Process Scheduling](#)

[7.5 Artificial Intelligence in Distributed Operating Systems](#)

[7.6 Current Progress](#)

[7.7 Quantum Artificial Intelligence](#)

[7.8 Conclusion](#)

[References](#)

[8 Techno-Nationalism and Techno-Globalization: A Perspective from the National Security Act](#)

[8.1 Introduction](#)

[8.2 Conclusion](#)

[Acknowledgement](#)

[References](#)

[9 Quantum Computing Based on Cybersecurity](#)

[9.1 Introduction](#)

[9.2 Preliminaries](#)

[9.3 Threat Landscape](#)

[9.4 Defensive Measurements, Countermeasures, and Best Practises](#)

[9.5 Conclusion](#)

[References](#)

[10 Quantum Cryptography for the Future Internet and the Security Analysis](#)

[10.1 Introduction](#)

[10.2 Related Works](#)

[10.3 Preliminaries](#)

[10.4 Quantum Cryptography for Future Internet](#)

[10.5 Conclusion](#)

[References](#)

[11 Security Aspects of Quantum Cryptography](#)

[11.1 Introduction](#)

[11.2 Literature Survey](#)

[11.3 Quantum Key Distribution](#)

[11.4 Cryptography](#)

[11.5 Quantum Cryptography with Faint Laser Pulses](#)

[11.6 Eavesdropping](#)

[11.7 Conclusion](#)

[References](#)

[12 Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses](#)

[12.1 Introduction](#)

[12.2 Quantum Computing Basics](#)

[12.3 Security Applications](#)

[12.4 Quantum Machine Learning](#)

[12.5 Conclusion](#)

[References](#)

13 Cyber Forensics and Cybersecurity: Threat Analysis, Research Statement and Opportunities for the Future

13.1 Introduction

13.2 Background

13.3 Scope of this Work

13.4 Methodology and Analysis of Simulation Results

13.5 Quantum-Based Cybersecurity and Forensics

13.6 Conclusion and Future Works

References

14 Quantum Computing: A Software Engineering Approach

14.1 Introduction

14.2 Background of Research Area

14.3 Why Cryptography?

14.4 Classical Cryptography

14.5 Quantum Cryptography (QCr)

14.6 Quantum Key Distribution

14.7 Cryptanalysis

14.8 Entanglement

14.9 Quantum Teleportation

14.10 Applications of QCr in Cybersecurity

14.11 Quantum Key Distribution Protocols Implementation

14.12 Research and Work

14.13 Challenges Faced by QC

14.14 Limitations

14.15 Conclusion

References

15 Quantum Computing to the Advantage of Neural Network

15.1 Introduction

15.2 Significance of Quantum Computers in Machine Learning

15.3 Related Work

15.4 Proposed Methodology

15.5 Result and Analysis

15.6 Conclusion

Glossary

References

16 Image Filtering Based on VQA with Quantum Security

16.1 Introduction

16.2 Related Work

16.3 Problem Statement

16.4 Working

16.5 Proposed Methodology Solution

16.6 Result Analysis

16.7 Conclusion

References

17 Quantum Computing Techniques Assessment and Representation

17.1 Introduction

17.2 Fundamentals of QC

17.3 Properties of QC

17.4 Topography of QC

17.5 The Architecture of QC

17.6 Quantum Algorithm

[17.7 Design Limitations of Quantum Computer](#)

[17.8 Different Categories of Quantum Computer](#)

[17.9 Advantages of QC](#)

[17.10 Disadvantages of QC](#)

[17.11 Applications of QC](#)

[17.12 Major Challenges in QC](#)

[17.13 Conclusion](#)

[References](#)

[18 Quantum Computing Technological Design Along with Its Dark Side](#)

[18.1 Introduction](#)

[18.2 Related Work](#)

[18.3 History and Evolution of QCOM](#)

[18.4 Components & Concepts that Make QCOM Possible](#)

[18.5 Plans for the Future Development of Quantum Computer](#)

[18.6 Dark Side of QCOM](#)

[18.7 Plans for Protection in Quantum Era](#)

[18.8 Conclusion](#)

[References](#)

[19 Quantum Technology for Military Applications](#)

[19.1 Introduction](#)

[19.2 Related Work](#)

[19.3 Overview of QTECH](#)

[19.4 QTECH in Defence](#)

[19.5 Military Applications of QTECH](#)

[19.6 Challenges and Consequences of Quantum Warfare](#)

[19.7 Conclusion](#)

[References](#)

[20 Potential Threats and Ethical Risks of Quantum Computing](#)

[20.1 Introduction](#)

[20.2 Research Design & Methodology](#)

[20.3 Brief In-Depth Overview of Possible Vulnerabilities](#)

[20.4 New Risks to be Created](#)

[20.5 Futuristic Picture of Quantum Ethics](#)

[20.6 Conclusion](#)

[References](#)

[21 Is Quantum Computing a Cybersecurity Threat?](#)

[21.1 Introduction](#)

[21.2 How QCom Threatens Cybersecurity](#)

[21.3 How QCom could Improve Cybersecurity](#)

[21.4 Quantum Cryptography and Its Applications](#)

[21.5 Proposed Methodology](#)

[21.6 Background/Objective](#)

[21.7 Conclusion](#)

[References](#)

[22 Quantum Computing in Data Security: A Critical Assessment](#)

[22.1 Introduction](#)

[22.2 Present Cryptographic Algorithms and Systems](#)

[22.3 Comparing Traditional Computing and Quantum Computing](#)

[22.4 Post-Quantum Cryptography \(PQC\)](#)

[22.5 Quantum Cryptography and Its Applications](#)

[22.6 Corporate Competitions Towards Quantum Computing](#)

[22.7 Threats Posed to Critical Infrastructure and Mechanisms](#)

[22.8 Conclusion](#)

[References](#)

[23 Quantum Computing and Security Aspects of Attention-Based Visual Question Answering with Long Short-Term Memory](#)

[23.1 Introduction](#)

[23.2 Literature Review](#)

[23.3 Problem Statement](#)

[23.4 Problem Elaboration](#)

[23.5 Proposed Methodology](#)

[23.6 Methods](#)

[23.7 Solution Approach](#)

[23.8 Expected Results](#)

[23.9 Conclusion](#)

[23.10 Abbreviations](#)

[References](#)

[24 Quantum Cryptography - A Security Architecture](#)

[24.1 Introduction](#)

[24.2 Related Work](#)

[24.3 Properties of Quantum Information](#)

[24.4 Methodology](#)

[24.5 Supported Explanation](#)

[24.6 Conclusion](#)

[References](#)

[25 Quantum Computing Anomalies in Communication](#)

[25.1 Introduction](#)

[25.2 Significance of Quantum Computing](#)

[25.3 The Dark Side of Quantum Computing](#)

[25.4 Previous Works](#)

[25.5 Conclusion](#)

[References](#)

[26 Intrusion Detection System via Classical SVM and Quantum SVM: A Comparative Overview](#)

[26.1 Introduction](#)

[26.2 Related Work](#)

[26.3 Models for IDS](#)

[26.4 Conclusion](#)

[References](#)

[27 Quantum Computing in Military Applications and Operations](#)

[27.1 Introduction](#)

[27.2 Literary Survey](#)

[27.3 Definition](#)

[27.4 Quantum Military Applications](#)

[27.5 Applications of QCRYP](#)

[27.6 Limitations](#)

[27.7 Conclusion](#)

[References](#)

[28 Quantum Cryptography Techniques: Evaluation](#)

[28.1 Introduction](#)

[28.2 Quantum Technology \(QTech\) in Defence](#)

[28.3 The QKD Model](#)

[28.4 Related Work](#)

[28.5 Preliminaries](#)

[28.6 QKD Protocols Implementation](#)

[28.7 Risk Analysis](#)

[28.8 Applications of Quantum Cryptography](#)

[28.9 Challenges of Quantum Cryptography](#)

[28.10 Conclusion and Future Work](#)

[References](#)

[29 Cyber Crime Attack Vulnerability Review for Quantum Computing](#)

[29.1 Introduction](#)

[29.2 Significance of Cyber Crime Attack for QC](#)

[29.3 Related Work](#)

[29.4 Proposed Methodology](#)

[29.5 Conclusion](#)

[References](#)

[About the Editors](#)

[Index](#)

[Also of Interest](#)

[End User License Agreement](#)

List of Tables

Chapter 2

[Table 2.1 Algorithm used to generate private key.](#)

Chapter 3

[Table 3.1 Traceback methods of DDoS attack.](#)

[Table 3.2 DDoS attacks, their effects and solutions \[28\].](#)

Chapter 4

[Table 4.1 Fivefold cross-validation scores for supervised learning models.](#)

[Table 4.2 Details of softmax function.](#)

[Table 4.3 Dataset samples with data attribute considered for quantum encoding....](#)

[Table 4.4 Categorization of the onion services with quantum encoding.](#)

Chapter 6

[Table 6.1 Performance characteristics for a speaker independent system.](#)

Chapter 10

[Table 10.1 Measurement result.](#)

Chapter 12

[Table 12.1 Augmented PCB defect dataset.](#)

[Table 12.2 CAE+QNN Architecture performance after 10 Epochs.](#)

Chapter 18

[Table 18.1 Evolution of Qubits over the years \[10, 11\].](#)

[Table 18.2 Comparison of investment of different countries in the development ...](#)

Chapter 22

[Table 22.1 Comparison of algorithms \[1-4\].](#)

Chapter 26

[Table 26.1 Comparison of different threats in Distributed Control Systems \[1,....](#)

Chapter 29

[Table 29.1 Comparison of different studies carried out for detection of differ...](#)

List of Illustrations

Chapter 1

[Figure 1.1 DDoS attack.](#)

[Figure 1.2 Quantum drones.](#)

Chapter 2

[Figure 2.1 Generalized properties of Quantum computation \[9\].](#)

[Figure 2.2 Quantum random walk on a circular walk \[17\].](#)

[Figure 2.3 Merkle tree structure \[23\].](#)

[Figure 2.4 Data security in the system.](#)

Chapter 3

[Figure 3.1 Working diagram of DDoS attack.](#)

[Figure 3.2 Remote DDoS attack classification.](#)

[Figure 3.3 Working of DDoS attack.](#)

[Figure 3.4 Cloud intrusion detection system for detecting the attacks \[28\].](#)

[Figure 3.5 Architecture of DDoS attack.](#)

[Figure 3.6 Classifications of DDoS attacks.](#)

Chapter 4

[Figure 4.1 Proposed methodology.](#)

[Figure 4.2 Softmax function.](#)

[Figure 4.3 Pseudocode of quantum encoding.](#)

[Figure 4.4 Quantum classification variational circuit.](#)

[Figure 4.5 Sample onion services.](#)

[Figure 4.6 Snapshot of sample cleaned text of onion service.](#)

[Figure 4.7 Categorization of different onion services.](#)

[Figure 4.8 Time required vs. Batch size of 2,000 onion services.](#)

[Figure 4.9 Memory required vs. batch size of 2000 URLs.](#)

Chapter 5

[Figure 5.1 Key components of the blockchain architecture.](#)

[Figure 5.2 Characteristics of the system.](#)

[Figure 5.3 Blockchain voting systems architectural overview.](#)

[Figure 5.4 Flow of the election process.](#)

[Figure 5.5 Use case diagram of the voting system.](#)

[Figure 5.6 npm install.](#)

[Figure 5.7 Running it by “node index.js”.](#)

[Figure 5.8 Run node index.js in terminal to run the project.](#)

[Figure 5.9 Create the smart contracts.](#)

[Figure 5.10 Linking Aadhaar card number to your phone number.](#)

[Figure 5.11 Testrpc showing the 10 accounts that can be used.](#)

[Figure 5.12 Deployment.](#)

[Figure 5.13 User registration.](#)

[Figure 5.14 Error message.](#)

[Figure 5.15 User login.](#)

[Figure 5.16 Aadhaar verification.](#)

[Figure 5.17 OTP on the user's Aadhaar linked phone number.](#)

[Figure 5.18 Error on wrong OTP.](#)

[Figure 5.19 Users casting their votes.](#)

[Figure 5.20 Blockchain transactions.](#)

Chapter 6

[Figure 6.1 Findings of the hidden coin-tossing test \[15, 16\].](#)

[Figure 6.2 An urn and ball model that demonstrates how a discrete symbol hidde...](#)

[Figure 6.3 Different HQMMs are depicted.](#)

[Figure 6.4 Connecting multiple contours for the usage of HQMMs for solitary wo...](#)

[Figure 6.5 The observed normalised duration density histograms for the 5 state...](#)

Chapter 8

[Figure 8.1 Techno-nationalism and techno-globalization.](#)

[Figure 8.2 Techno-nationalism concept framework: implications for MNEs.](#)

Chapter 9

[Figure 9.1 Architecture of quantum computing.](#)

Chapter 10

[Figure 10.1 Quantum direct communication model.](#)

[Figure 10.2 Quantum teleportation.](#)

[Figure 10.3 Classical communication model.](#)

[Figure 10.4 Model of QKD protocol.](#)

[Figure 10.5 QKD protocol in noise-free channel.](#)

[Figure 10.6 QKD protocol with 30% noise.](#)

[Figure 10.7 The effect of eavesdropping on the rate of error.](#)

[Figure 10.8 The eavesdropper detects the channel with different probability.](#)

Chapter 11

[Figure 11.1 Key distribution pattern of basic quantum \[9, 10\].](#)

Chapter 12

[Figure 12.1 Hybrid quantum-classical architecture as an example.](#)

[Figure 12.2 The network architecture of CAE + QNN.](#)

[Figure 12.3 \(a\) Original PCB image of size 600 × 600 \(b\) Cropped defect image ...](#)

Chapter 13

[Figure 13.1 Percentage of businesses compromised by at least one cyberattack....](#)

[Figure 13.2 Percentage of organization hit by at least one successful ransomwa...](#)

Chapter 15

[Figure 15.1 \(a\) A qubit state \$|\psi\rangle\$ represented on a bloch sphere \[1, 2\]. \(b\) Ga...](#)

[Figure 15.2 Models of conventional and quantum learning are shown schematicall...](#)

[Figure 15.3 QC ANN with qubits as nodes of the network using hybrid quantum-cl...](#)

[Figure 15.4 Cost vs. number of training steps of Classical ANN and QC ANN usin...](#)

Chapter 16

[Figure 16.1 Visual Question Answering \[4, 5, 12\].](#)

[Figure 16.2 Identifying the image \[1, 2\].](#)

[Figure 16.3 RSA internal working \[1, 6\].](#)

[Figure 16.4 Typical RSA algorithm working \[6, 7\].](#)

[Figure 16.5 Visual AI system \[5, 6\].](#)

[Figure 16.6 Image of fingerprint \[2, 3, 5-7, 12, 14\].](#)

Chapter 17

[Figure 17.1 Difference between classical computer and quantum computer \[4\].](#)

[Figure 17.2 Architecture of quantum computing \[5\].](#)

Chapter 20

[Figure 20.1 The difference between traditional computers and quantum computers...](#)

[Figure 20.2 The specificity of keywords majorly displayed \[7, 8\].](#)

[Figure 20.3 Potential threats or security vulnerability causes \[3, 4\].](#)

[Figure 20.4 How vulnerability increases as we go down to the stack for differe...](#)

[Figure 20.5 How the quantum technologies are being expanded \[2, 3\].](#)

Chapter 21

[Figure 21.1 Symmetric cryptography \[1-3\].](#)

[Figure 21.2 Public key cryptography \[4-6\].](#)

[Figure 21.3 Classical and quantum cryptography \[5, 7, 8\].](#)

[Figure 21.4 Public key cryptography in action \[1, 2, 6-8\].](#)

Chapter 22

[Figure 22.1 Demonstration of classical cryptography \[1-4\].](#)

[Figure 22.2 Circuit for state preparation for 2 qubits and 4-dimensional input...](#)

[Figure 22.3 N quantum particle interactions with the environment to implement ...](#)

[Figure 22.4 Comparison of various symmetric algorithms \[3, 5, 50, 51\].](#)

[Figure 22.5 Comparison of channels \[62, 63\].](#)

Chapter 23

[Figure 23.1 Att.-based LSTM functioning from label encoding to prediction and ...](#)

[Figure 23.2 RW demonstration of VQA system using dual-key-MM BD threats \[15\]....](#)

[Figure 23.3 A simple illustration of visual question answering \(VQA\) system wo...](#)

[Figure 23.4 Overview of a design VAQ MM system with complete PP of BD thefts \[...](#)

[Figure 23.5 Customer question answer visual to demonstrate problem of E-Commer...](#)

[Figure 23.6 Demonstration of BD attack situation initiated by attacker to brea...](#)

[Figure 23.7 \(a\) objective function. \(b\) VT patches configured with some flower...](#)

[Figure 23.8 Demonstration of the internal process of the VQA system with atten...](#)

Chapter 24

[Figure 24.1 QCom: basic layout \[1-4\].](#)

[Figure 24.2 Quantum cryptography implementation architecture \[20, 21\].](#)

[Figure 24.3 Quantum ratio: key_generation \[7, 8\].](#)

[Figure 24.4 Flow process computing \[9, 10\].](#)

[Figure 24.5 Attackers action over message, using keys \[11, 12\].](#)

Chapter 25

[Figure 25.1 Quantum computing and the future of big data \[1, 2\].](#)

[Figure 25.2 Diving deep into quantum computing \[3, 4\].](#)

[Figure 25.3 Applications of quantum computing \[5, 6, 12\].](#)

Chapter 26

[Figure 26.1 \(a\) Visualization of Qubits. \(b\) Visualization of Qubits.](#)

[Figure 26.2 Classical SVM separating parameters \[16, 17, 19, 20\].](#)

[Figure 26.3 Q-SVM \(Quantum SVM\) \[1, 2, 15, 17, 18\].](#)

Chapter 27

[Figure 27.1 Quantum computing model \[1, 2\].](#)

[Figure 27.2 The quantum teleportation \[7, 8\].](#)

[Figure 27.3 Quantum key distribution model \[5, 11\].](#)

[Figure 27.4 Quantum warfare \[3, 12, 13\].](#)

[Figure 27.5 Spending on Qcom by country \[14, 15\].](#)

Chapter 28

[Figure 28.1 Symbols for photons state - 1st \[1, 2\].](#)

[Figure 28.2 Symbols for photons state - 2nd \[3, 4\].](#)

[Figure 28.3 Quantum key distribution \[2, 5-7\].](#)

[Figure 28.4 Quantum direct communication model \[1, 2, 8, 9\].](#)

[Figure 28.5 Quantum teleportation \[1-3, 8, 10, 11\].](#)

[Figure 28.6 The QKD protocol stack \[1, 2, 12-15\].](#)

[Figure 28.7 The Design Stack \[1, 3, 5\].](#)

Chapter 29

[Figure 29.1 A QC architecture \[1, 5\].](#)

[Figure 29.2 Sources of cybercrime attacks \[7-9\].](#)

[Figure 29.3 Ideal time required to decrypt each algorithm using brute force at...](#)

[Figure 29.4 Public key cryptography in action \[6, 18\].](#)

[Figure 29.5 Entire communication process using QKD and classical protocols \[6, ...](#)

[Figure 29.6 Hacker attempting to crack the private key \[6\].](#)

[Figure 29.7 Hacker attempting to retrieve the private key using QC Setup with ...](#)

[Figure 29.8 Quantum key distribution server setup \[6\].](#)

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

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.