

1. Record Nr.	UNINA9910841889103321
Autore	Tyagi Amit Kumar
Titolo	Automated Secure Computing for Next-Generation Systems
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2024 ©2024
ISBN	1-394-21394-8 1-394-21392-1
Edizione	[1st ed.]
Descrizione fisica	1 online resource (468 pages)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Preface -- Acknowledgements -- Part 1: Fundamentals -- Chapter 1 Digital Twin Technology: Necessity of the Future in Education and Beyond -- 1.1 Introduction -- 1.2 Digital Twins in Education -- 1.2.1 Virtual Reality for Immersive Learning -- 1.2.2 Delivery of Remote Education -- 1.2.3 Replication of Real-World Scenarios -- 1.2.4 Promote Intelligences and Personalization -- 1.3 Examples and Case Studies -- 1.3.1 Examples of DTT in Education -- 1.3.2 Digital Twin-Based Educational Systems -- 1.4 Discussion -- 1.5 Challenges and Limitations -- 1.5.1 Technical Challenges -- 1.5.2 Pedagogical Challenges -- 1.5.3 Ethical and Privacy Concerns -- 1.5.4 Future Research Directions -- 1.6 Conclusion -- References -- Chapter 2 An Intersection Between Machine Learning, Security, and Privacy -- 2.1 Introduction -- 2.2 Machine Learning -- 2.2.1 Overview of Machine Learning -- 2.2.2 Machine Learning Stages: Training and Inference -- 2.3 Threat Model -- 2.3.1 Attack Model of Machine Learning -- 2.3.2 Trust Model -- 2.3.3 Machine Learning Capabilities in a Differential Environment -- 2.3.4 Opposite Views of Machine Learning in Security -- 2.4 Training in a Differential Environment -- 2.4.1 Achieving Integrity -- 2.5 Inferring in Adversarial Attack -- 2.5.1 Combatants in the White Box Model -- 2.5.2 Insurgencies in the Black Box Model -- 2.6 Machine Learning Methods That Are Sustainable, Private, and Accountable -- 2.6.1 Robustness of

Models to Distribution Drifts -- 2.6.2 Learning and Inferring With Privacy -- 2.6.3 Fairness and Accountability in Machine Learning -- 2.7 Conclusion -- References -- Chapter 3 Decentralized, Distributed Computing for Internet of Things-Based Cloud Applications -- 3.1 Introduction to Volunteer Edge Cloud for Internet of Things Utilising Blockchain.

3.2 Significance of Volunteer Edge Cloud Concept -- 3.3 Proposed System -- 3.3.1 Smart Contract -- 3.3.2 Order Task Method -- 3.3.3 KubeEdge -- 3.4 Implementation of Volunteer Edge Control -- 3.4.1 Formation of a Cloud Environment -- 3.5 Result Analysis of Volunteer Edge Cloud -- 3.6 Introducing Blockchain-Enabled Internet of Things Systems Using the Serverless Cloud Platform -- 3.7 Introducing Serverless Cloud Platforms -- 3.7.1 IoT Systems -- 3.7.2 JointCloud -- 3.7.3 Computing Without Servers -- 3.7.4 Oracle and Blockchain Technology -- 3.8 Serverless Cloud Platform System Design -- 3.8.1 Aim and Constraints -- 3.8.2 Goals and Challenges -- 3.8.3 HCloud Connections -- 3.8.4 Data Sharing Platform -- 3.8.5 Cloud Manager -- 3.8.6 The Agent -- 3.8.7 Client Library -- 3.8.8 Witness Blockchain -- 3.9 Evaluation of HCloud -- 3.9.1 CPU Utilization -- 3.9.2 Cost Analysis -- 3.10 HCloud-Related Works -- 3.10.1 Serverless -- 3.10.2 Efficiency -- 3.11 Conclusion -- References -- Chapter 4 Artificial Intelligence-Blockchain-Enabled-Internet of Things-Based Cloud Applications for Next-Generation Society -- 4.1 Introduction -- 4.2 Background Work -- 4.3 Motivation -- 4.4 Existing Innovations in the Current Society -- 4.5 Expected Innovations in the Next-Generation Society -- 4.6 An Environment with Artificial Intelligence-Blockchain-Enabled-Internet of Things-Based Cloud Applications -- 4.7 Open Issues in Artificial Intelligence-Blockchain-Enabled-Internet of Things-Based Cloud Applications -- 4.8 Research Challenges in Artificial Intelligence-Blockchain-Enabled-Internet of Things-Based Cloud Applications -- 4.9 Legal Challenges in Artificial Intelligence-Blockchain-Enabled-Internet of Things-Based Cloud Applications -- 4.10 Future Research Opportunities Towards Artificial Intelligence-Blockchain-Enabled-Internet of Things-Based Cloud Applications. 4.11 An Open Discussion -- 4.12 Conclusion -- References -- Chapter 5 Artificial Intelligence for Cyber Security: Current Trends and Future Challenges -- 5.1 Introduction: Security and Its Types -- 5.1.1 Human Aspects of Information Security -- 5.2 Network and Information Security for Industry 4.0 and Society 5.0 -- 5.2.1 Industry 4.0 vs Society 5.0 -- 5.2.2 Industry 4.0 to Society 5.0 -- 5.3 Internet Monitoring, Espionage, and Surveillance -- 5.4 Cyber Forensics with Artificial Intelligence and without Artificial Intelligence -- 5.5 Intrusion Detection and Prevention Systems Using Artificial Intelligence -- 5.6 Homomorphic Encryption and Cryptographic Obfuscation -- 5.7 Artificial Intelligence Security as Adversarial Machine Learning -- 5.8 Post-Quantum Cryptography -- 5.9 Security and Privacy in Online Social Networks and Other Sectors -- 5.10 Security and Privacy Using Artificial Intelligence in Future Applications/Smart Applications -- 5.11 Security Management and Security Operations Using Artificial Intelligence for Society 5.0 and Industry 4.0 -- 5.11.1 Implementation on the Internet of Things and Protecting Data in IoT Connected Devices -- 5.12 Digital Trust and Reputation Using Artificial Intelligence -- 5.13 Human-Centric Cyber Security Solutions -- 5.14 Artificial Intelligence-Based Cyber Security Technologies and Solutions -- 5.15 Open Issues, Challenges, and New Horizons Towards Artificial Intelligence and Cyber Security -- 5.15.1 An Overview of Cyber-Security -- 5.15.2 The Role of Artificial Intelligence in Cyber Security -- 5.15.3 AI Is Continually Made Smarter -- 5.15.4 AI Never Misses a Day

of Work -- 5.15.5 AI Swiftly Spots the Threats -- 5.15.6 Impact of AI on Cyber Security -- 5.15.7 AI in Cyber Security Case Study -- 5.16 Future Research with Artificial Intelligence and Cyber Security -- 5.17 Conclusion -- References.

Part 2: Methods and Techniques -- Chapter 6 An Automatic Artificial Intelligence System for Malware Detection -- 6.1 Introduction -- 6.2 Malware Types -- 6.3 Structure Format of Binary Executable Files -- 6.4 Malware Analysis and Detection -- 6.5 Malware Techniques to Evade Analysis and Detection -- 6.6 Malware Detection With Applying AI -- 6.7 Open Issues and Challenges -- 6.8 Discussion and Conclusion -- References -- Chapter 7 Early Detection of Darknet Traffic in Internet of Things Applications -- 7.1 Introduction -- 7.2 Literature Survey -- 7.3 Proposed Work -- 7.3.1 Drawback -- 7.4 Analysis of the Work -- 7.5 Future Work -- 7.6 Conclusion -- References -- Chapter 8 A Novel and Efficient Approach to Detect Vehicle Insurance Claim Fraud Using Machine Learning Techniques -- 8.1 Introduction -- 8.2 Literature Survey -- 8.3 Implementation and Analysis -- 8.3.1 Dataset Description -- 8.3.2 Methodology -- 8.3.3 Checking for Missing Values -- 8.3.4 Exploratory Data Analysis -- 8.4 Conclusion -- 8.4.1 Future Work -- 8.4.2 Limitations -- References -- Chapter 9 Automated Secure Computing for Fraud Detection in Financial Transactions -- 9.1 Introduction -- 9.2 Historical Perspective -- 9.3 Previous Models for Fraud Detection in Financial Transactions -- 9.3.1 CatBoost -- 9.3.2 XGBoost -- 9.3.3 LightGBM -- 9.4 Proposed Model Based on Automated Secure Computing -- 9.5 Discussion -- 9.6 Conclusion -- References -- Additional Readings -- Chapter 10 Data Anonymization on Biometric Security Using Iris Recognition Technology -- 10.1 Introduction -- 10.2 Problems Faced in Facial Recognition -- 10.3 Face Recognition -- 10.4 The Important Aspects of Facial Recognition -- 10.5 Proposed Methodology -- 10.6 Results and Discussion -- 10.7 Conclusion -- References -- Chapter 11 Analysis of Data Anonymization Techniques in Biometric Authentication System. 11.1 Introduction -- 11.2 Literature Survey -- 11.3 Existing Survey -- 11.3.1 Biometrics Technology -- 11.3.2 Palm Vein Authentication -- 11.3.3 Methods of Palm Vein Authentication -- 11.3.4 Limitations of the Existing System -- 11.4 Proposed System -- 11.4.1 Biometric System -- 11.4.2 Data Processing Technique -- 11.4.3 Data-Preserving Approach -- 11.4.3.1 Generalization -- 11.4.3.2 Suppression -- 11.4.3.3 Swapping -- 11.4.3.4 Masking -- 11.5 Implementation of AI -- 11.6 Limitations and Future Works -- 11.7 Conclusion -- References -- Part 3: Applications -- Chapter 12 Detection of Bank Fraud Using Machine Learning Techniques -- 12.1 Introduction -- 12.2 Literature Review -- 12.3 Problem Description -- 12.4 Implementation and Analysis -- 12.4.1 Workflow -- 12.4.2 Dataset -- 12.4.3 Methodology -- 12.5 Results -- 12.6 Conclusion -- 12.7 Future Works -- References -- Chapter 13 An Internet of Things-Integrated Home Automation with Smart Security System -- 13.1 Introduction -- 13.2 Literature Review -- 13.3 Methodology and Working Procedure with Diagrams -- 13.4 Research Analysis -- 13.5 Establishment of the Prototype -- 13.6 Results and Discussions -- 13.7 Conclusions -- Acknowledgment -- References -- Chapter 14 An Automated Home Security System Using Secure Message Queue Telemetry Transport Protocol -- 14.1 Introduction -- 14.2 Related Works -- 14.2.1 PIR Home Security Solutions -- 14.2.2 Solutions for MQTT Security -- 14.2.3 Solutions for Home Automation -- 14.3 Proposed Solution -- 14.3.1 Technological Decisions -- 14.3.2 Hardware Decision -- 14.3.3 Module Overview -- 14.4 Implementation -- 14.5 Results -- 14.6 Conclusion and Future Work -- References -- Chapter 15 Machine Learning-Based Solutions

for Internet of Things-Based Applications -- 15.1 Introduction -- 15.2
IoT Ecosystem -- 15.2.1 IoT Devices -- 15.2.2 IoT Gateways -- 15.2.3
IoT Platforms.
15.2.4 IoT Applications.
