1. Record Nr. UNINA9910366655603321

Titolo	Handbook of Computer Networks and Cyber Security : Principles and Paradigms / / edited by Brij B. Gupta, Gregorio Martinez Perez, Dharma P. Agrawal, Deepak Gupta
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	9783030222772 3030222772
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (xx, 959 pages) : illustrations
Disciplina	004.6
Soggetti	Data protection Computer networks Computers Artificial intelligence Security Computer Communication Networks Information Systems and Communication Service Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1. Security Frameworks in Mobile Cloud Computing -- 2. An investigation study of Privacy Preserving in Cloud -- 3. Towards new quantitative security risk analysis models for information systems: A Cloud Computing case study -- 4. A Novel AckIBE based Secure Cloud Data Management Framework -- 5. A Practicable Machine Learning Solution for Security-cognizant Data Placement on Cloud Platforms -- 6. Threats behind default configurations of network devices: local network attacks and their countermeasures -- 7. Security and Privacy issues in Wireless Sensor and Body Area Networks -- 8. Preventing Security and Privacy Attacks in WBANs -- 9. Security in Underwater Wireless Sensor Networks -- 10. Security Issues in Cognitive Radio Ad Hoc Networks -- 11. Security and privacy in social networks: Data and Structural Anonymity -- 12. SOI FinFET for Computer Networks and

Cyber Security Systems -- 13. Software Defined Networking: An Innovative Approach to Computer Networks -- 14. Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions -- 15. Survey on DDoS Attacks Techniques and Solutions in Software Defined Network -- 16. Classification of Cooperative Distributed Denial of Service Defense (DDoS) Schemes -- 17. Epidemic Modelling for the Spread of Bots through DDoS Attack in E-Commerce Network -- 18. Physical unclonable functions (puf) based security in iot: key challenges and solutions -- 19. Fog Computing: Applications and Secure Data Aggregation -- 20. A Comprehensive review of Distributed Denial of service (DDoS) Attacks in Fog Computing Environment -- 21. Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network -- 22. Heterogeneous-Internet of Vehicles (IoV) Communication in 21st Century: A comprehensive study -- 23. A Systematic Review on Security and Privacy Issues in Mobile Devices and Systems -- 24. Investigation of Security Issues in Distributed Systems Monitoring -- 25. An analysis of Provable Security Frameworks for RFID Security -- 26. Computational Techniques for Real Time Credit Card Fraud Detection -- 27. Requirements, Protocols and Security Challenges in Wireless Sensor Networks - An Industrial Perspective -- 28. Privacy Preservation of Electronic Health Record: Current Status and Future Direction -- 29. QKD protocols security between theory and engineering implementation -- 30. Survey of Security and Privacy issues on Biometric system -- 31. A Novel Session key Generation and Secure Communication Establishment Protocol Using Fingerprint Biometrics -- 32. Trees, CryptoSignatures and Cyberspace Mobile Agent Interfaces -- 33. Permutation-Substitution Based Image Encryption Algorithms using Pseudo Random Number Generators -- 34. Recent Trends in Document Authentication using Text Steganography -- 35. Machine Learning Based Intrusion Detection Techniques -- 36. Feature Selection using a Machine Learning to Classify a Malware -- 37. DeepDGA-MINet: Cost-Sensitive Deep Learning based Framework for Handling Multiclass Imbalanced DGA Detection -- 38. ABFT: Analytics to uplift Big Social Events Using Forensic Tools -- 39. HackIt: A Real-Time Simulation Tool for Studying Real-World Cyber-Attacks in the Laboratory.

Sommario/riassunto

This handbook introduces the basic principles and fundamentals of cyber security towards establishing an understanding of how to protect computers from hackers and adversaries. The highly informative subject matter of this handbook, includes various concepts, models, and terminologies along with examples and illustrations to demonstrate substantial technical details of the field. It motivates the readers to exercise better protection and defense mechanisms to deal with attackers and mitigate the situation. This handbook also outlines some of the exciting areas of future research where the existing approaches can be implemented. Exponential increase in the use of computers as a means of storing and retrieving security-intensive information, requires placement of adequate security measures to safeguard the entire computing and communication scenario. With the advent of Internet and its underlying technologies, information security aspects are becoming a prime concern towards protecting the networks and the cyber ecosystem from variety of threats, which is illustrated in this handbook. This handbook primarily targets professionals in security, privacy and trust to use and improve the reliability of businesses in a distributed manner, as well as computer scientists and software developers, who are seeking to carry out research and develop software in information and cyber security. Researchers and advanced-level students in computer science will also benefit from this reference.