1. Record Nr. UNINA9910767586503321

Autore	Qureshi Kashif Naseer
Titolo	Cybersecurity Vigilance and Security Engineering of Internet of Everything / / edited by Kashif Naseer Qureshi, Thomas Newe, Gwanggil Jeon, Abdellah Chehri
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-45162-7
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (229 pages)
Collana	Internet of Things, Technology, Communications and Computing, , 2199-1081
Altri autori (Persone)	NeweThomas JeonGwanggil ChehriAbdellah
Disciplina	621.382
Soggetti	Telecommunication Cooperating objects (Computer systems) Internet of things Security systems Communications Engineering, Networks Cyber-Physical Systems Internet of Things Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Part A: Security Threats and Vulnerabilities -- Internet of Everything: Evolution and fundamental concepts -- Cybersecurity Threats and Attacks in IoE Networks -- Attacks Detection Mechanism for IoE Networks -- Cyber Resilience, Principles, and Practices -- Future Cybersecurity Challenges for IoE Networks -- Part B: Security Vigilance and Security Engineering for IoE Networks -- Networking and Security Architectures for IoE Networks -- Machine Learning-Based Detection and Prevention Systems for IoE -- Role of Blockchain Models for IoE Infrastructures and Applications -- Cybersecurity as a Service -- Big data Analytics for Cybersecurity in IoE Networks -- Cybersecurity Standards and Policies for CPS in IoE -- Future Privacy, and Trust Challenges for IoE Networks -- Conclusion.

Sommario/riassunto

This book first discusses cyber security fundamentals then delves into security threats and vulnerabilities, security vigilance, and security engineering for Internet of Everything (IoE) networks. After an introduction, the first section covers the security threats and vulnerabilities or techniques to expose the networks to security attacks such as repudiation, tampering, spoofing, and elevation of privilege. The second section of the book covers vigilance or prevention techniques like intrusion detection systems, trust evaluation models, crypto, and hashing privacy solutions for IoE networks. This section also covers the security engineering for embedded and cyber-physical systems in IoE networks such as blockchain, artificial intelligence, and machine learning-based solutions to secure the networks. This book provides a clear overview in all relevant areas so readers gain a better understanding of IoE networks in terms of security threats, prevention, and other security mechanisms. Discusses cyber security threats and vulnerabilities, security vigilance, and security engineering for IoE networks; Provides prevention techniques like intrusion detection, trust evaluation, crypto, and hashing privacy solutions; Features tips to secure networks from security attacks like repudiation, tampering, spoofing, and elevation of privilege.