1. Record Nr. UNINA9910878973803321

| | |
|---|---|
| Autore | Alaba Fadele Ayotunde |
| Titolo | Security Framework and Defense Mechanisms for IoT Reactive Jamming Attacks / / by Fadele Ayotunde Alaba, Alvaro Rocha |
| Pubbl/distr/stampa | Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024 |
| ISBN | 9783031659294<br>9783031659287 |
| Edizione | [1st ed. 2024.] |
| Descrizione fisica | 1 online resource (128 pages) |
| Collana | Studies in Systems, Decision and Control, , 2198-4190 ; ; 548 |
| Altri autori (Persone) | RochaAlvaro |
| Disciplina | 621 |
| Soggetti | Security systems<br>Engineering mathematics<br>Engineering - Data processing<br>Security Science and Technology<br>Mathematical and Computational Engineering Applications<br>Data Engineering |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | 1. Introduction -- 2.Internet of Things -- 3.Embedded IoT Security Framework -- 4.Defense Mechanism for Reactive Jamming Attack in IoT Networks -- 5.Statistical Results Validation -- 6.Conclusions and Future Directions. |
| Sommario/riassunto | This book digs into the important confluence of cybersecurity and big data, providing insights into the ever-changing environment of cyber threats and solutions to protect these enormous databases. In the modern digital era, large amounts of data have evolved into the vital organs of businesses, providing the impetus for decision-making, creativity, and a competitive edge. Cyberattacks pose a persistent danger to this important resource since they can result in data breaches, financial losses, and harm to an organization's brand. Features of particular interest include: a. Understanding the Threat Landscape: The book gives a complete review of the many different types of cyber threats that target big data, including data breaches, ransomware attacks, and insider threats. b. Analysing Real-World Case Studies: The purpose of this section is to provide the reader with useful |

insights into the strategies, methods, and processes that cyber adversaries use via the in-depth examination of real-world assaults on big data. c. Strategies for Risk Mitigation: This book provides a comprehensive and actionable approach to reducing the dangers of cyberattacks on large amounts of data. It encompasses a broad variety of tactics, including network protection, encoding, and access restrictions d. Emerging Technologies: This section introduces readers to cutting-edge technologies and best practices for securing large data. e. Compliance with Regulations: The book examines the regulatory environment that governs data protection and privacy, including the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and industry-specific requirements. f. Trends of the Future: This book covers current trends and issues in cybersecurity and gives forward-looking views into the future of big data security. This is done in recognition that the cybersecurity environment is always shifting and developing. g. Contributors of Expertise: The book includes contributions from industry practitioners, data scientists, and cybersecurity specialists who have hands-on experience defending large data settings.