

1. Record Nr.	UNINA9911007469103321
Titolo	6G Cyber Security Resilience: Trends and Challenges // edited by H. L. Gururaj, VinayaKumar Ravi, J. Shreyas, N. Pavithra, R. Sapna
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-85008-4
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (VIII, 262 p. 60 illus., 54 illus. in color.)
Collana	Advanced Sciences and Technologies for Security Applications, , 2363-9466
Disciplina	005.8
Soggetti	Data protection Artificial intelligence Quantum computers Security systems Data and Information Security Artificial Intelligence Quantum Computing Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Analysis and Comparison of Various Steganography Methods for secure 6G communication -- Image Encryption in the Compressed Domain using Autoencoders for 6G communication -- The Security Design and Challenges of 6G Architecture -- Cyber Security technologies for Privacy in 6G Networks -- Advancements in AI and ML for Enhanced Security and Performance in 6G Networks -- ML-Driven Secure Communication for Next-Generation 6G Networks -- Building a Better Network: The Promising Future of 6G Technology Applications and Challenges -- Building a Better Network: The Promising Future of 6G Technology Applications and Challenges -- Blockchain and Distributed Ledger Technology for 6G Security -- 6G Cyber Security Resilience: Trends and Challenges -- IoT and Edge Computing Security: Essential Aspects of 6G Networks -- Enhancing Cyber security in 6G Networks with Federated Learning for Collaborative Threat Mitigation -- Federated Learning for Enhancing Cybersecurity in IoT-Integrated 6G

Sommario/riassunto

This book offers a comprehensive analysis of intersection of significant domains, including information security, 6G technology, and cybersecurity. This reference work addresses gaps in existing literature by providing insights, research findings, and personal evaluations from esteemed scholars in the field. Holographic-type communications (HTC), tactile Internet, connected autonomous vehicles (CAVs), unmanned aerial vehicles (UAVs), autonomous healthcare solutions, manufacturing systems, and virtual/augmented/extended reality (VR/AR/XR), along with other cutting-edge applications, will continue to advance with the advent of 6G. The advent of the 6G era has been ushered in by the rapid advancement of communication technologies, promising unprecedented applications and connectivity. As we venture into this unexplored domain, the criticality of cybersecurity resilience cannot be overstated. This book examines and assesses the emerging trends in 6G technology, with a particular focus on the intricate challenges encountered in the realm of cybersecurity. By analyzing the intricate interplay between IoT integration, AI/ML security, quantum communication, and the intricacies of the physical layer, this book endeavors to provide a comprehensive understanding of the perpetually evolving threat landscape. It is reasonable to expect that 6G, similar to its predecessors, will promote advancements in the domain of connectivity and telecommunications through the provision of increased data throughput, decreased latency, and expanded capacity. These developments will promote the development of innovative applications and services, thus increasing the importance of robust cybersecurity protocols. As 6G technology continues to proliferate, it becomes increasingly vital to ensure the security and preservation of data. The primary audience of this book is industrialists, academicians, researchers, and UG/PG students. The secondary audience consists of practitioners, cyberpolice, lawmakers, legal firms, etc. as we are also covering regulatory and ethical considerations in 6G cybersecurity.
