1. Record Nr. UNINA9910999687103321

Titolo	Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics / / edited by Faisal Rehman, Inam Ullah Khan, Oroos Arshi, Shashi Kant Gupta
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-81481-9
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XIV, 203 p. 56 illus., 51 illus. in color.)
Collana	Information Systems Engineering and Management, , 3004-9598 ; ; 32
Disciplina	620.00285
Soggetti	Engineering - Data processing Computational intelligence Artificial intelligence Data Engineering Computational Intelligence Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1.AI-Driven Modern Cybersecurity Approach: A Systematic Literature Review -- 2.Cyber Security in the Post-Quantum Computer Era: Threats and Perspectives -- 3.Deep Neural Network for DoS Detection in Wireless Sensors Networks.-4.Survey on IoT Security Threats Application and Architectures -- 5.Lightweight Cryptography Algorithms for IoT Devices -- 6.Guarding the Digital Gateway: An In-depth Analysis of Cybersecurity Challenges in India -- 7.Predictive Modeling for Food Security Assessment Using Synthetic Minority Over-Sampling Technique -- 8.Exploring the Secure Unleashing of Digital Potential: A Study on How Cloud Security Works Together with Digital Transformation in Financial Institutions of Pakistan -- 9.Reviewing Theoretical Perspectives on IT Governance and Compliance in Banking: Insights from US Regulatory Frameworks -- 10.Overcoming Challenges and Implementing Effective Information Security Policies for Remote Work Environments -- 11.Generative Adversarial Networks (GAN) Insights for Cyber Security Applications -- 12.Future Emerging Challenges and Innovations in Next Gen-Cybersecurity and Information

Systems Security.

Sommario/riassunto

This book is a comprehensive exploration into the intersection of cutting-edge technologies and the critical domain of cybersecurity; this book delves deep into the evolving landscape of cyber threats and the imperative for innovative solutions. From establishing the fundamental principles of cyber security to scrutinizing the latest advancements in AI and machine learning, each chapter offers invaluable insights into bolstering defenses against contemporary threats. Readers are guided through a journey that traverses the realms of cyber analytics, threat analysis, and the safeguarding of information systems in an increasingly interconnected world. With chapters dedicated to exploring the role of AI in securing IoT devices, employing supervised and unsupervised learning techniques for threat classification, and harnessing the power of recurrent neural networks for time series analysis, this book presents a holistic view of the evolving cybersecurity landscape. Moreover, it highlights the importance of next-generation defense mechanisms, such as generative adversarial networks (GANs) and federated learning techniques, in combating sophisticated cyber threats while preserving privacy. This book is a comprehensive guide to integrating AI and data science into modern cybersecurity strategies. It covers topics like anomaly detection, behaviour analysis, and threat intelligence, and advocates for proactive risk mitigation using AI and data science. The book provides practical applications, ethical considerations, and customizable frameworks for implementing next-gen cyber defense strategies. It bridges theory with practice, offering real-world case studies, innovative methodologies, and continuous learning resources to equip readers with the knowledge and tools to mitigate cyber threats.