1.	Record Nr.	UNINA9910869181403321
	Autore	Chen Yingying
	Titolo	Network Security Empowered by Artificial Intelligence / / edited by Yingying Chen, Jie Wu, Paul Yu, Xiaogang Wang
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
	ISBN	9783031535109 9783031535093
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (443 pages)
	Collana	Advances in Information Security, , 2512-2193 ; ; 107
	Altri autori (Persone)	WuJie YuPaul WangXiaogang
	Disciplina	006.3
	Soggetti	Artificial intelligence Computer networks - Security measures Machine learning Artificial Intelligence Mobile and Network Security Machine Learning
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Preface -- Part I. Architecture Innovations and Security in 5G Networks -- Chapter. 1. nCore: Clean Slate Next-G Mobile Core Network Architecture for Scalability and Low Latency -- Chapter. 2. Decision-Dominant Strategic Defense Against Lateral Movement for 5G Zero-Trust Multi-Domain Networks -- Part. II. Security in Artificial Intelligence-enabled Intrusion Detection Systems -- Chapter. 3. Artificial Intelligence and Machine Learning for Network Security – Quo Vadis? -- Chapter 4. Understanding the Ineffectiveness of the Transfer Attack in Intrusion Detection System -- Chapter. 5. Advanced ML/DL-based Intrusion Detection Systems for Software-Defined Networks -- Part III. Attack and Defense in Artificial Intelligence-enabled Wireless Systems -- Chapter. 6. Deep Learning for Robust and Secure Wireless Communications -- Chapter. 7. Universal Targeted Adversarial Attacks Against mmWave-based Human Activity Recognition -- Chapter. 8. AdversarialMachine Learning for Wireless Localization -- Chapter. 9.

Sommario/riassunto

This book introduces cutting-edge methods on security in spectrum management, mobile networks and next-generation wireless networks in the era of artificial intelligence (AI) and machine learning (ML). This book includes four parts: (a) Architecture Innovations and Security in 5G Networks, (b) Security in Artificial Intelligence-enabled Intrusion Detection Systems. (c) Attack and Defense in Artificial Intelligence-enabled Wireless Systems, (d) Security in Network-enabled Applications. The first part discusses the architectural innovations and security challenges of 5G networks, highlighting novel network structures and strategies to counter vulnerabilities. The second part provides a comprehensive analysis of intrusion detection systems and the pivotal role of AI and machine learning in defense and vulnerability assessment. The third part focuses on wireless systems, where deep learning is explored to enhance wireless communication security. The final part broadens the scope, examining the applications of these emerging technologies in network-enabled fields. The advancement of AI/ML has led to new opportunities for efficient tactical communication and network systems, but also new vulnerabilities. Along this direction, innovative AI-driven solutions, such as game-theoretic frameworks and zero-trust architectures are developed to strengthen defenses against sophisticated cyber threats. Adversarial training methods are adopted to augment this security further. Simultaneously, deep learning techniques are emerging as effective tools for securing wireless communications and improving intrusion detection systems. Additionally, distributed machine learning, exemplified by federated learning, is revolutionizing security model training. Moreover, the integration of AI into network security, especially in cyber-physical systems, demands careful consideration to ensure it aligns with the dynamics of these systems. This book is valuable for academics, researchers, and students in AI/ML, network security, and related fields. It serves as a resource for those in computer networks, AI, ML, and data science, and can be used as a reference or secondary textbook.