1.	Record Nr.	UNINA9910770257603321
	Autore	Gunjan Vinit Kumar
	Titolo	Modern Approaches in IoT and Machine Learning for Cyber Security [[electronic resource]] : Latest Trends in AI / / edited by Vinit Kumar Gunjan, Mohd Dilshad Ansari, Mohammed Usman, ThiDieuLinh Nguyen
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
	ISBN	3-031-09955-9
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (415 pages)
	Collana	Internet of Things, Technology, Communications and Computing, , 2199-1081
	Altri autori (Persone)	AnsariMohd Dilshad UsmanMohammed (Electrical engineering professor) NguyenThiDieuLinh
	Disciplina	005.8
	Soggetti	Cooperating objects (Computer systems) Telecommunication Data protection Quantitative research Cyber-Physical Systems Communications Engineering, Networks Data and Information Security Data Analysis and Big Data
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Introduction -- Being secure, vigilant and resilient in the age of Industry 4.0 -- Facing new cyber risks in the age of smart production -- Leveraging AI for threat detection -- Being resilient when attacks inevitably hit home -- Security for the Industrial Internet of Things -- Reinventing the Internet to Secure the Digital Economy -- The future of cybersecurity -- Adapting data science for security challenges -- Big data analytics for cybersecurity -- Data Analytics and Decision Support for Cybersecurity -- Data Science in Cybersecurity and Cyberthreat Intelligence -- Integrating cyber security and data science for social media -- Data warehousing and data mining techniques for cyber security -- Machine learning and deep learning methods for

cybersecurity -- Machine Learning and Big Data Processing for Cybersecurity Data Analysis -- Blockchain's roles in strengthening cybersecurity and protecting privacy -- Using virtual environments for the assessment of cybersecurity issues in IoT scenarios -- Security considerations for secure and trustworthy smart home system in the IoT environment -- Cyber security challenges for IoT-based smart grid networks -- Evaluating critical security issues of the IoT world -- Internet of Things security and forensics -- Applying Artificial Intelligence Techniques to Prevent Cyber Assaults -- Cyber security and the role of intelligent systems in addressing its challenges -- Cyber security of water SCADA systems -- Bio-inspiring cyber security and cloud services -- AI enabled blockchain smart contracts -- Cyber security and the evolution in intrusion detection systems -- A cyber security study of a SCADA energy management system -- Security analysis and recommendations for AI/ML enabled automated cyber medical systems -- Making knowledge tradable in edge-AI enabled IoT -- Artificial intelligence and national security -- Conclusion.

Sommario/riassunto

This book examines the cyber risks associated with Internet of Things (IoT) and highlights the cyber security capabilities that IoT platforms must have in order to address those cyber risks effectively. The chapters fuse together deep cyber security expertise with artificial intelligence (AI), machine learning, and advanced analytics tools, which allows readers to evaluate, emulate, outpace, and eliminate threats in real time. The book’s chapters are written by experts of IoT and machine learning to help examine the computer-based crimes of the next decade. They highlight on automated processes for analyzing cyber frauds in the current systems and predict what is on the horizon. This book is applicable for researchers and professionals in cyber security, AI, and IoT. Examines cyber risks associated with IoT and highlights essential cyber security capabilities needed to address risks effectively; Fuses deep cyber security expertise with artificial intelligence, machine learning and advanced analytics tools; Includes a case study about an automated process for analyzing cyber frauds specifically in phishing and cloning.