1. Record Nr.	UNISA996464508903316
Titolo	AI-enabled threat detection and security analysis for industrial IoT / / Hadis Karimipour, Farnaz Derakhshan, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-76613-6
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (VIII, 250 p. 94 illus., 82 illus. in color.)
Disciplina	005.8
Soggetti	Internet of things - Security measures Computer security Artificial intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Artificial Intelligence for Threat Detection and Analysis in Industrial IoT: Applications and Challenges -- Complementing IIoT Services through AI: Feasibility and Suitability -- Data Security and Privacy in Industrial IoT -- Blockchain Applications in the Industrial Internet of Things -- Application of Deep Learning on IoT-enabled Smart Grid Monitoring -- Cyber Security of Smart Manufacturing Execution Systems: A Bibliometric Analysis -- The Role of Machine Learning in IIoT Through FPGAs -- Deep Representation Learning for Cyber-Attack Detection in Industrial IoT -- Classification and Intelligent Mining of Anomalies in Industrial IoT -- A Snapshot Ensemble Deep Neural Network Model for Attack Detection in Industrial Internet of Things -- Privacy Preserving Federated Learning Solution for Security of Industrial Cyber Physical Systems -- A Multi-Stage Machine Learning Model for Security Analysis in Industrial Control System -- A Recurrent Attention Model for Cyber Attack Classification.
Sommario/riassunto	This contributed volume provides the state-of-the-art development on security and privacy for cyber-physical systems (CPS) and industrial Internet of Things (IIoT). More specifically, this book discusses the security challenges in CPS and IIoT systems as well as how Artificial Intelligence (AI) and Machine Learning (ML) can be used to address

these challenges. Furthermore, this book proposes various defence strategies, including intelligent cyber-attack and anomaly detection algorithms for different IIoT applications. Each chapter corresponds to an important snapshot including an overview of the opportunities and challenges of realizing the AI in IIoT environments, issues related to data security, privacy and application of blockchain technology in the IIoT environment. This book also examines more advanced and specific topics in AI-based solutions developed for efficient anomaly detection in IIoT environments. Different AI/ML tecniques including deep representation learning, Snapshot Ensemble Deep Neural Network (SEDNN), federated learning and multi-stage learning are discussed and analysed as well. Researchers and professionals working in computer security with an emphasis on the scientific foundations and engineering techniques for securing IIoT systems and their underlying computing and communicating systems will find this book useful as a reference. The content of this book will be particularly useful for advanced-level students studying computer science, computer technology, cyber security, and information systems. It also applies to advanced-level students studying electrical engineering and system engineering, who would benefit from the case studies.