1. Record Nr. UNINA9910632476503321

Titolo	Artificial Intelligence for Cyber-Physical Systems Hardening / / edited by Issa Traore, Isaac Woungang, Sherif Saad
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	3-031-16237-4
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (241 pages)
Collana	Engineering Cyber-Physical Systems and Critical Infrastructures, , 2731-5010 ; ; 2
Disciplina	060 006.3
Soggetti	Cooperating objects (Computer systems) Engineering - Data processing Computational intelligence Big data Artificial intelligence Cyber-Physical Systems Data Engineering Computational Intelligence Big Data Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Introduction -- Machine Learning Construction: implications to cybersecurity -- Machine Learning Assessment: implications to cybersecurity -- A Collection of Datasets for Intrusion Detection in MIL-STD-1553 Platforms -- Unsupervised Anomaly Detection for MIL-STD-1553 Avionic Platforms using CUSUM -- Secure Design of Cyber-Physical Systems at the Radio Frequency Level: Machine and Deep Learning-Driven Approaches, Challenges and Opportunities -- Attack Detection by Using Deep Learning for Cyber-Physical System -- Security and privacy of IoT devices for ageing in place -- Detecting Malicious Attacks Using Principal Component Analysis in Medical Cyber-Physical Systems -- Activity and Event Network Graph and

Application to Cyberphysical Security.

Sommario/riassunto

This book presents advances in security assurance for cyber-physical systems (CPS) and report on new machine learning (ML) and artificial intelligence (AI) approaches and technologies developed by the research community and the industry to address the challenges faced by this emerging field. Cyber-physical systems bridge the divide between cyber and physical-mechanical systems by combining seamlessly software systems, sensors, and actuators connected over computer networks. Through these sensors, data about the physical world can be captured and used for smart autonomous decision-making. This book introduces fundamental AI/ML principles and concepts applied in developing secure and trustworthy CPS, disseminates recent research and development efforts in this fascinating area, and presents relevant case studies, examples, and datasets. We believe that it is a valuable reference for students, instructors, researchers, industry practitioners, and related government agencies staff.