1. Record Nr.   UNINA9910731481703321

   Autore   Sarveshwaran Velliangiri

   Titolo   Artificial Intelligence and Cyber Security in Industry 4.0 / / edited by
                        Velliangiri Sarveshwaran, Joy Iong-Zong Chen, Danilo Pelusi

   Pubbl/distr/stampa   Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2023

   ISBN   981-9921-15-5

   Edizione   [1st ed. 2023.]

   Descrizione fisica   1 online resource (374 pages)

   Collana   Advanced Technologies and Societal Change, , 2191-6861

   Altri autori (Persone) ChenJoy Iong-zong
                           PelusiDanilo

   Disciplina   658.4038028563

   Soggetti   Artificial intelligence
                        Internet of things
                        Big data
                        Machine learning
                        Computational intelligence
                        Wireless communication systems
                        Mobile communication systems
                        Artificial Intelligence
                        Internet of Things
                        Big Data
                        Machine Learning
                        Computational Intelligence
                        Wireless and Mobile Communication

   Lingua di pubblicazione Inglese

   Formato   Materiale a stampa

   Livello bibliografico Monografia

   Nota di contenuto   Introduction to Artificial Intelligence and Cyber Security for Industry --
                        Role of AI and its impact on the development of cyber security
                        applications -- AI and IoT in Manufacturing and related Security
                        Perspectives for Industry 4.0 -- IoT Security Vulnerabilities and
                        Defensive Measures in Industry 4.0 -- Adopting Artificial Intelligence in
                        ITIL for Information Security Management - Way forward in Industry 4.0
                        -- Intelligent Autonomous Drones in Industry 4.0 -- A review on
                        automatic generation of attack trees and its application to automotive
                        cybersecurity -- Malware Analysis using Machine Learning Tools and

Techniques in IT Industry -- USE OF MACHINE LEARNING IN FORENSICS AND COMPUTER SECURITY -- Control of feed drives in CNC machine tools using artificial immune adaptive strategy -- Efficient Anomaly Detection for Empowering Cyber Security by Using Adaptive Deep Learning Model -- Intrusion Detection in IoT based Healthcare Using ML and DL approaches: A Case Study -- War Strategy Algorithm based GAN model for Detecting the Malware Attacks in Modern Digital Age -- ML algorithms for providing financial security in banking sectors with the prediction of loan risks -- Machine Learning based DDoS Attack Detection using Support Vector Machine -- Artificial Intelligence based Cyber Security Applications.

Sommario/riassunto	This book provides theoretical background and state-of-the-art findings in artificial intelligence and cybersecurity for industry 4.0 and helps in implementing AI-based cybersecurity applications. Machine learning-based security approaches are vulnerable to poison datasets which can be caused by a legitimate defender's misclassification or attackers aiming to evade detection by contaminating the training data set. There also exist gaps between the test environment and the real world. Therefore, it is critical to check the potentials and limitations of AI-based security technologies in terms of metrics such as security, performance, cost, time, and consider how to incorporate them into the real world by addressing the gaps appropriately. This book focuses on state-of-the-art findings from both academia and industry in big data security relevant sciences, technologies, and applications.