1. Record Nr. UNINA9910770267403321

Autore	Wang Cliff
Titolo	AI Embedded Assurance for Cyber Systems / / edited by Cliff Wang, S.S. Iyengar, Kun Sun
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	9783031426377 3031426371
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (252 pages)
Altri autori (Persone)	IyengarS. S SunKun
Disciplina	006.3
Soggetti	Computational intelligence Computer networks - Security measures Artificial intelligence Computer crimes Cooperating objects (Computer systems) Computational Intelligence Mobile and Network Security Artificial Intelligence Computer Crime Cybercrime Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part. I. AI/ML for Digital Forensics -- Chapter. 1. Writer-dependent Off-line Signature Verification with Neural Networks -- Chapter. 2. Political Activism and Technology -- Chapter. 3. Forensic Proof and Criminal Liability for Development, Distribution and Use of Artificial Intelligence -- Part. II. AI/ML for CPS -- Chapter. 4. Automotive Batteries as Anomaly Detectors -- Chapter. 5. Zero Trust Architecture For Cyber-Physical Power System Security Based on Machine Learning -- Chapter. 6. AI-enabled Real-time Sensor Attack Detection for Cyber-physical Systems -- Part. III. AI/ML for Cyber Analysis -- Chapter. 7. Generating

Vulnerable Code via Learning-Based Program Transformation -- Chapter. 8. Security and Privacy Problems in Self-Supervised Learning -- Chapter. 9. Federated Learning for IoT Applications, Attacks and Defense Methods -- Chapter. 10. AI Powered Correlation Technique to Detect VirtualMachine Attacks in Private Cloud Environment -- Chapter. 11. Detecting Fake Users in Online Social Networks -- Chapter. 12. Explaining Deep Learning based Security Applications -- Glossary -- Index.

Sommario/riassunto

The rapid growth and reliance on cyber systems have permeated our society, government, and military which is demonstrated in this book. The authors discuss how AI-powered cyber systems are designed to protect against cyber threats and ensure the security and reliability of digital systems using artificial intelligence (AI) technologies. As AI becomes more integrated into various aspects of our lives, the need for reliable and trustworthy AI systems becomes increasingly important. This book is an introduction to all of the above-mentioned areas in the context of AI Embedded Assurance for Cyber Systems. This book has three themes. First, the AI/ML for digital forensics theme focuses on developing AI and ML powered forensic tools, techniques, software, and hardware. Second, the AI/ML for cyber physical system theme describes that AI/ML plays an enabling role to boost the development of cyber physical systems (CPS), especially in strengthening the security and privacy ofCPS. Third, the AI/ML for cyber analysis theme focuses on using AI/ML to analyze tons of data in a timely manner and identify many complex threat patterns. This book is designed for undergraduates, graduate students in computer science and researchers in an interdisciplinary area of cyber forensics and AI embedded security applications. It is also useful for practitioners who would like to adopt AIs to solve cyber security problems.