1. Record Nr.	UNINA9910349287503321
Titolo	Deep Learning Applications for Cyber Security / / edited by Mamoun Alazab, MingJian Tang
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-13057-6
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (260 pages)
Collana	Advanced Sciences and Technologies for Security Applications, , 1613-5113
Disciplina	005.8
Soggetti	Big data Computer crimes Neural networks (Computer science) Computer security System safety Big Data Cybercrime Mathematical Models of Cognitive Processes and Neural Networks Systems and Data Security Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Adversarial Attack, Defense, and Applications with Deep Learning Frameworks -- Intelligent Situational-Awareness Architecture for Hybrid Emergency Power Systems in More Electric Aircraft -- Deep Learning in Person Re-identication for Cyber-Physical Surveillance Systems -- Deep Learning-based Detection of Electricity Theft Cyber-attacks in Smart Grid AMI Networks -- Using Convolutional Neural Networks for Classifying Malicious Network Traffic -- DBD: Deep Learning DGA-based Botnet Detection -- Enhanced Domain Generating Algorithm Detection Based on Deep Neural Networks -- Intrusion Detection in SDN-based Networks: Deep Recurrent Neural Network Approach -- SeqDroid: Obfuscated Android Malware Detection using Stacked Convolutional and Recurrent Neural Networks -- Forensic

Detection of Child Exploitation Material using Deep Learning -- Toward Detection of Child Exploitation Material: A Forensic Approach.

Sommario/riassunto

Cybercrime remains a growing challenge in terms of security and privacy practices. Working together, deep learning and cyber security experts have recently made significant advances in the fields of intrusion detection, malicious code analysis and forensic identification. This book addresses questions of how deep learning methods can be used to advance cyber security objectives, including detection, modeling, monitoring and analysis of as well as defense against various threats to sensitive data and security systems. Filling an important gap between deep learning and cyber security communities, it discusses topics covering a wide range of modern and practical deep learning techniques, frameworks and development tools to enable readers to engage with the cutting-edge research across various aspects of cyber security. The book focuses on mature and proven techniques, and provides ample examples to help readers grasp the key points. .