1. Record Nr. UNINA9910488713403321

Autore	Chen Xiaofeng
Titolo	Cyber Security Meets Machine Learning / / edited by Xiaofeng Chen, Willy Susilo, Elisa Bertino
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2021
ISBN	981-336-726-1
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (168 pages)
Disciplina	006.31
Soggetti	Data protection Machine learning Image processing - Digital techniques Computer vision Database management Computer networks Application software Data and Information Security Machine Learning Computer Imaging, Vision, Pattern Recognition and Graphics Database Management System Computer Communication Networks Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1. IoT Attacks and Malware -- Chapter 2. Machine Learning-based Online Source Identification for Image Forensics -- Chapter 3. Reinforcement Learning Based Communication Security for Unmanned Aerial Vehicles -- Chapter 4. Visual Analysis of Adversarial Examples in Machine Learning -- Chapter 5. Adversarial Attacks against Deep Learning-based Speech Recognition Systems -- Chapter 6. Secure Outsourced Machine Learning -- Chapter 7. A Survey on Secure Outsourced Deep Learning.
Sommario/riassunto	Machine learning boosts the capabilities of security solutions in the modern cyber environment. However, there are also security concerns

associated with machine learning models and approaches: the vulnerability of machine learning models to adversarial attacks is a fatal flaw in the artificial intelligence technologies, and the privacy of the data used in the training and testing periods is also causing increasing concern among users. This book reviews the latest research in the area, including effective applications of machine learning methods in cybersecurity solutions and the urgent security risks related to the machine learning models. The book is divided into three parts: Cyber Security Based on Machine Learning; Security in Machine Learning Methods and Systems; and Security and Privacy in Outsourced Machine Learning. Addressing hot topics in cybersecurity and written by leading researchers in the field, the book features self-contained chapters to allow readers to select topics that are relevant to their needs. It is a valuable resource for all those interested in cybersecurity and robust machine learning, including graduate students and academic and industrial researchers, wanting to gain insights into cutting-edge research topics, as well as related tools and inspiring innovations.