1. Record Nr. UNINA9910847583403321

Autore	Guerraoui Rachid
Titolo	Robust Machine Learning : Distributed Methods for Safe AI / / by Rachid Guerraoui, Nirupam Gupta, Rafael Pinot
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2024
ISBN	981-9706-88-2
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (0 pages)
Collana	Machine Learning: Foundations, Methodologies, and Applications, , 2730-9916
Disciplina	006.3
Soggetti	Machine learning Computer security Multiagent systems Cloud computing Machine Learning Principles and Models of Security Multiagent Systems Cloud Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Chapter 1. Context & Motivation -- Chapter 2. Basics of Machine Learning -- Chapter 3. Federated Machine Learning -- Chapter 4. Fundamentals of Robust Machine Learning -- Chapter 5. Optimal Robustness -- Chapter 6. Practical Robustness. .
Sommario/riassunto	Today, machine learning algorithms are often distributed across multiple machines to leverage more computing power and more data. However, the use of a distributed framework entails a variety of security threats. In particular, some of the machines may misbehave and jeopardize the learning procedure. This could, for example, result from hardware and software bugs, data poisoning or a malicious player controlling a subset of the machines. This book explains in simple terms what it means for a distributed machine learning scheme to be robust to these threats, and how to build provably robust machine learning algorithms. Studying the robustness of machine learning algorithms is a necessity given the ubiquity of these algorithms in both

the private and public sectors. Accordingly, over the past few years, we have witnessed a rapid growth in the number of articles published on the robustness of distributed machine learning algorithms. We believe it is time to provide a clear foundation to this emerging and dynamic field. By gathering the existing knowledge and democratizing the concept of robustness, the book provides the basis for a new generation of reliable and safe machine learning schemes. In addition to introducing the problem of robustness in modern machine learning algorithms, the book will equip readers with essential skills for designing distributed learning algorithms with enhanced robustness. Moreover, the book provides a foundation for future research in this area. .