1. Record Nr. UNINA9910993945703321

Autore	Li Jin
Titolo	Privacy-Preserving Machine Learning / / by Jin Li, Ping Li, Zheli Liu, Xiaofeng Chen, Tong Li
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2022
ISBN	9789811691393 9811691398 9789811691386 981169138X
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (VIII, 88 p. 21 illus., 18 illus. in color.)
Collana	SpringerBriefs on Cyber Security Systems and Networks, , 2522-557X
Disciplina	005.8 323.448
Soggetti	Data protection - Law and legislation Machine learning Privacy Machine Learning
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Secure Cooperative Learning in Early Years -- Outsourced Computation for Learning -- Secure Distributed Learning -- Learning with Differential Privacy -- Applications - Privacy-Preserving Image Processing -- Threats in Open Environment -- Conclusion.
Sommario/riassunto	This book provides a thorough overview of the evolution of privacy-preserving machine learning schemes over the last ten years, after discussing the importance of privacy-preserving techniques. In response to the diversity of Internet services, data services based on machine learning are now available for various applications, including risk assessment and image recognition. In light of open access to datasets and not fully trusted environments, machine learning-based applications face enormous security and privacy risks. In turn, it presents studies conducted to address privacy issues and a series of proposed solutions for ensuring privacy protection in machine learning tasks involving multiple parties. In closing, the book reviews state-of-

the-art privacy-preserving techniques and examines the security threats they face.