1. Record Nr. UNISA996418217803316

Titolo	Federated learning : privacy and incentive / / edited by Qiang Yang, Lixin Fan, and Han Yu
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] Â©2020
ISBN	3-030-63076-5
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (X, 286 p. 94 illus., 82 illus. in color.)
Collana	Lecture Notes in Artificial Intelligence ; ; 12500
Disciplina	006.31
Soggetti	Federated database systems Application software Machine learning
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Privacy -- Threats to Federated Learning -- Rethinking Gradients Safety in Federated Learning -- Rethinking Privacy Preserving Deep Learning: How to Evaluate and Thwart Privacy Attacks -- Task-Agnostic Privacy-Preserving Representation Learning via Federated Learning -- Large-Scale Kernel Method for Vertical Federated Learning -- Towards Byzantine-resilient Federated Learning via Group-wise Robust Aggregation -- Federated Soft Gradient Boosting Machine for Streaming Data -- Dealing with Label Quality Disparity In Federated Learning -- Incentive -- FedCoin: A Peer-to-Peer Payment System for Federated Learning -- Efficient and Fair Data Valuation for Horizontal Federated Learning -- A Principled Approach to Data Valuation for Federated Learning -- A Gamified Research Tool for Incentive Mechanism Design in Federated Learning -- Budget-bounded Incentives for Federated Learning -- Collaborative Fairness in Federated Learning -- A Game-Theoretic Framework for Incentive Mechanism Design in Federated Learning -- Applications -- Federated Recommendation Systems -- Federated Learning for Open Banking -- Building ICU In-hospital Mortality Prediction Model with Federated Learning -- Privacy-preserving Stacking with Application to Cross-organizational Diabetes Prediction. .

Sommario/riassunto

This book provides a comprehensive and self-contained introduction to Federated Learning, ranging from the basic knowledge and theories to various key applications, and the privacy and incentive factors are the focus of the whole book. This book is timely needed since Federated Learning is getting popular after the release of the General Data Protection Regulation (GDPR). As Federated Learning aims to enable a machine model to be collaboratively trained without each party exposing private data to others. This setting adheres to regulatory requirements of data privacy protection such as GDPR. This book contains three main parts. First, it introduces different privacy-preserving methods for protecting a Federated Learning model against different types of attacks such as Data Leakage and/or Data Poisoning. Second, the book presents incentive mechanisms which aim to encourage individuals to participate in the Federated Learning ecosystems. Last but not the least, this book also describes how Federated Learning can be applied in industry and business to address data silo and privacy-preserving problems. The book is intended for readers from both academia and industries, who would like to learn federated learning from scratch, practice its implementation, and apply it in their own business. Readers are expected to have some basic understanding of linear algebra, calculus, and neural network. Additionally, domain knowledge in FinTech and marketing are preferred.