

1. Record Nr.	UNINA9910584601303321
Titolo	Federated Learning : A Comprehensive Overview of Methods and Applications // edited by Heiko Ludwig, Nathalie Baracaldo
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-030-96896-0
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (vi, 534 pages) : illustrations
Disciplina	006.31
Soggetti	Artificial intelligence Machine learning Artificial Intelligence Machine Learning
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Introduction to Federated Learning -- Tree-Based Models for Federated Learning Systems -- Semantic Vectorization: Text and Graph-Based Models -- Personalization in Federated Learning -- Personalized, Robust Federated Learning with Fed+ -- Communication-Efficient Distributed Optimization Algorithms -- Communication-Efficient Model Fusion -- Federated Learning and Fairness -- Introduction to Federated Learning Systems -- Local Training and Scalability of Federated Learning Systems -- Straggler Management -- Systems Bias in Federated Learning -- Protecting Against Data Leakage in Federated Learning: What Approach Should You Choose? -- Private Parameter Aggregation for Federated Learning -- Data Leakage in Federated Learning -- Security and Robustness in Federated Machine Learning -- Dealing with Byzantine Threats to Neural Networks -- Privacy-Preserving Vertical Federated Learning -- Split Learning: A Resource Efficient Model & Data Parallel Approach for Distributed Deep Learning -- Federated Learning for Collaborative Financial Crimes Detection -- Federated Reinforcement Learning for Portfolio Management -- Application of Federated Learning in Medical Imaging -- Advancing Healthcare Solutions with Federated Learning -- A Privacy-preserving Product Recommender System -- Application of Federated Learning in

Federated Learning: A Comprehensive Overview of Methods and Applications presents an in-depth discussion of the most important issues and approaches to federated learning for researchers and practitioners. Federated Learning (FL) is an approach to machine learning in which the training data are not managed centrally. Data are retained by data parties that participate in the FL process and are not shared with any other entity. This makes FL an increasingly popular solution for machine learning tasks for which bringing data together in a centralized repository is problematic, either for privacy, regulatory or practical reasons. This book explains recent progress in research and the state-of-the-art development of Federated Learning (FL), from the initial conception of the field to first applications and commercial use. To obtain this broad and deep overview, leading researchers address the different perspectives of federated learning: the core machine learning perspective, privacy and security, distributed systems, and specific application domains. Readers learn about the challenges faced in each of these areas, how they are interconnected, and how they are solved by state-of-the-art methods. Following an overview on federated learning basics in the introduction, over the following 24 chapters, the reader will dive deeply into various topics. The first part addresses algorithmic questions of solving different machine learning tasks in a federated way and how to train efficiently, at scale, and fairly. Another part focuses on providing clarity on how to select privacy and security solutions in a way that can be tailored to specific use cases, while another considers the pragmatics of the systems where the federated learning process will run. The book also covers other important use cases for federated learning, such as split learning and vertical federated learning. Finally, the book includes some chapters focusing on applying FL in real-world enterprise settings.
