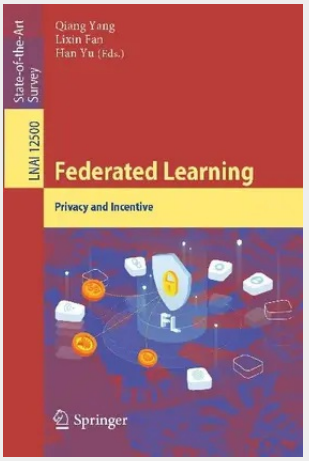
Yang / Fan / Yu

Federated Learning

Privacy and Incentive



This book provides a comprehensive and self-contained introduction to federated learning, ranging from the basic knowledge and theories to various key applications. Privacy and incentive issues are the focus of this book. It is timely as federated learning is becoming popular after the release of the General Data Protection Regulation (GDPR). Since 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. Firstly, 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. Secondly, the book presents incentive mechanisms which aim to encourage individuals to participate in the federated learning ecosystems. Last but not 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 the academia and the industry, who would like to learn about federated learning, 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 would be helpful."

This book provides a comprehensive and self-contained introduction to federated learning, ranging from the basic knowledge and theories to various key applications. Privacy and incentive issues are the focus of this book. It is timely as federated learning is becoming popular after the release of the General Data Protection Regulation (GDPR). Since 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. Firstly, 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. Secondly, the book presents incentive mechanisms which aim to encourage individuals to participate in the federated learning ecosystems. Last but not 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 the academia and the industry, who would like to learn about federated learning, 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 would be helpful."

90,94 €
84,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030630751
Medium: Buch
ISBN: 978-3-030-63075-1
Verlag: Palgrave Macmillan
Erscheinungstermin: 26.11.2020
Sprache(n): Englisch
Auflage: 1. Auflage 2020
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 452 g
Seiten: 286
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)