Lecture Notes in Artificial Intelligence 12500

Subseries of Lecture Notes in Computer Science

More information about this subseries at http://www.springer.com/series/1244

Qiang Yang · Lixin Fan · Han Yu (Eds.)

Federated Learning

Privacy and Incentive

Springer

Editors
Qiang Yang
WeBank
Shenzhen, China

Lixin Fan
WeBank
Shenzhen, China

Hong Kong University of Science
and Technology
Hong Kong, Hong Kong

Han Yu
Nanyang Technological University
Singapore, Singapore

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Artificial Intelligence
ISBN 978-3-030-63075-1 ISBN 978-3-030-63076-8 (eBook)
https://doi.org/10.1007/978-3-030-63076-8

LNCS Sublibrary: SL7 – Artificial Intelligence

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Machine learning (ML) has shown significant potential for revolutionizing many important applications such as fraud detection in finance, medical diagnosis in healthcare, or speech recognition in automatic customer service. The traditional approach of training ML models requires large-scale datasets. However, with rising public concerns for data privacy protection, such an approach is facing tremendous challenges. Trust establishment techniques such as blockchains can help users ascertain the origin of the data and audit their usage. Nevertheless, we still require a viable approach to extract value from such trustworthy data and fairly distribute such values to promote collaboration.

Federated learning (FL) is an emerging ML paradigm that aims to help the field of ML adapt to and thrive under the new normal of heightened data privacy concerns and distributively owned data silos. It offers a promising alternative to enable multiple participants to train a globally shared model by exchanging model information without exposing private data.

The protection of data *privacy* is often mandated by the regulatory requirements (e.g., GDPR) in business-to-consumer scenarios. Violations of such regulations can incur hefty fines amounting to the billions. Moreover, in business-to-business settings, participants from the same business sectors may be competitors. This poses further unique challenges for the design of federated *incentives* to fairly account for their contributions and sustain collaboration in the presence of competition. Research works pertaining data privacy protection and incentive mechanism design under FL settings are crucial for the formation and healthy development of FL ecosystems. This is what makes FL unique compared to existing distributed ML paradigms. Therefore, our book focuses on these two main themes.

Although FL training processes are decentralized, without exposing private data, one crux of data privacy protection is to avoid the shared model parameters being exploited by potential adversaries. In this book, we have collected multiple studies on privacy-preserving ML to show the readers potential approaches that can strengthen the privacy aspect of FL.

Despite a wealth of literature on incentive mechanism design exists, the unique settings and challenges facing FL requires meaningful extensions to these approaches. In this book, we have gathered multiple studies on motivating participants to join FL training through rewards (monetary or otherwise) in order to build a sustainable FL ecosystem.

Knowing the theories and techniques about privacy preservation and incentivization under FL is one thing, but successfully applying them in practice also requires non-trivial effort. In this book, we have also included a number of studies on the application of FL in important fields such as recommendation systems and banking.

This book consists of 19 chapters, each of which is a single-blind peer-reviewed submission. Most of the chapters are extensions from workshop or conference

contributions. By providing a well-balanced collection of recent works on *privacy*, *incentive* and the *applications* of FL, the book can help readers gain a more nuanced understanding on how to build a robust and sustainable FL ecosystem and translate the research outcomes into real-world impact. The book is therefore expected to be useful for academic researchers, FL system developers as well as people interested in advanced artificial intelligence topics.

Last but not least, we would like to express our gratitude towards our amazing colleagues, specially Lanlan Chang and Jian Li from the Springer team. Without their help, the publication of this book would not be possible.

September 2020

Qiang Yang
Lixin Fan
Han Yu

Organization

Editorial Team

Qiang Yang	WeBank, China, and The Hong Kong University of Science and Technology, Hong Kong
Lixin Fan	WeBank, China
Han Yu	Nanyang Technological University, Singapore

Program Committee

Kam Woh Ng	WeBank, China
Yilun Jin	The Hong Kong University of Science and Technology, Hong Kong
Tianyu Zhang	WeBank, China

Contents

Privacy

Incentive