Editorial

Introduction to the Special Issue on Federated Machine Learning

Yang Liu
Webank

Han Yu
Nanyang Technological University

Qiang Yang
Webank and Hong Kong University of Science and Technology

Federated Learning (FL), a.k.a. federated machine learning, is an emerging research paradigm focusing on solving data-silos challenges in real-world industrial applications. It is a broad discipline that touches many topics, including distributed and collaborative learning, privacy-preserving machine learning, edge computing, and data valuation, etc. Its interdisciplinary nature calls for collaborative efforts from a variety of fields to establish new protocols, frameworks and systems to address unique challenges, and open problems. This special issue highlights a selection of high-quality and original works in this new area, including accepted papers to the 1st International Workshop on Federated Machine Learning in conjunction with IJCAI 2019. In this special issue, the following papers will provide the interested readers with a variety of topics to get their bearings around this emerging field.

1. Huadi Zheng, Haibo Hu, and Ziyang Han, "Preserving User Privacy for Machine Learning: Local Differential Privacy or Federated Machine Learning?," reported a useful study to compare the efficiency and privacy-preserving properties achievable by LDP and FL in IoT applications.
2. Chi Zhang, Yu Liu, Le Wang, Yuehu Liu, Li Li, and Nanning Zheng, "Joint Intelligence Ranking by Federated Multiplicative Update," proposed a privacy-preserving matrix factorization method which has potential applicability in many intelligent systems such as autonomous driving.
3. Yang Liu, Qingchen Liu, Xiong Zhang, Shuqi Qin, and Xiaoping Lei, "Distributed Privacy-Preserving Iterative Summation Protocols," developed a distributed iterative protocol for privacy preservation which is resilient to

Digital Object Identifier 10.1109/MIS.2020.3014704
Date of current version 3 September 2020.

Published by the IEEE Computer Society

dynamic joining and leaving of nodes. It can be a useful enabling technique to enhance privacy protection in dynamic FL systems.

4. Kun Zhao, Wei Xi, Zhi Wang, Ruimeng Wang, Zhiping Jiang, and Jizhong Zhao, "SMSS: Secure Member Selection Strategy in Federated Learning," seek to address the issue of diverse data quality from data owners by selecting those with more common entities to join FL model training.
5. Aleksei Triastcyn and Boi Faltings, "Federated Generative Privacy," focus on the issue of privacy-preserving data sharing. They proposed GAN-based approach to generate artificial data samples to support federated averaging operations without disclosing sensitive local information.
6. Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, and Qiang Yang, "A Sustainable Incentive Scheme for Federated Learning," focus on the important issue of incentive mechanism design in FL settings. They developed a fairness-aware profit-sharing scheme to motivate participation by data owners in federated learning.
7. Yang Liu, Yan Kang, Chaoping Xing, Tianjian Chen, and Qiang Yang, "A Secure Federated Transfer Learning Framework," proposed the first federated transfer learning method to help FL application deal with challenging situations in which overlaps in the sample space and the feature space are both rare.
8. Based on the federated transfer learning framework, Yiqiang Chen, Xin Qin, Jindong Wang, Chaohui Yu, and Wen Gao, "FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare," reported their experience applying the FTL in the healthcare application domain.
9. Han Cha, Jihong Park, Hyesung Kim, Mehdi Bennis, and Seong-Lyun Kim, "Proxy Experience Replay: Federated Distillation for Distributed Reinforcement Learning," proposed an approach to enhance communication efficiency and preserve private information in distributed deep reinforcement learning.

Looking forward, federated learning is undergoing rapid growth as a new research area. After it has been first introduced by Google,[1] federated learning has witnessed tremendous growth of interest from both academia and industry.[2,3] Recently, authors from Webank published the first monograph on federated learning.[4] Companies and institutions have joined the IEEE P3652.1 Federated Machine Learning Working Group to establish the first industrial standard on federated learning frameworks. Federated learning has been applied in financial, healthcare and other business scenarios to overcome data barriers.[5] Driven by an increasing demand for data collaboration, future work on federated learning would not only consider system and algorithm related topics, but also fairness, privacy, and legal aspects, making federated learning a multilevel interdisciplinary paradigm.

REFERENCES

1. H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist.*, 2017, pp. 1273–1282.
2. Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 12:1–12:19, 2019.
3. P. Kairouz *et al.*, "Advances and open problems in federated learning," 2019, *arXiv:1912.04977*[cs.LG].
4. Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, *Federated Learning*. San Rafael, CA, USA: Morgan & Claypool, 2019.
5. The FATE Authors. Federated AI Technology Enabler, 2019. [Online]. Available: https://www.fedai.org/