IEEE Transactions on Neural Networks and Learning Systems (IEEE TNNLS) Special Issue on Trustworthy Federated Learning

Introduction

As AI becomes ubiquitous with advances in AI research, the key barrier to AI adoption is no longer technical in nature. Instead, it is often more about gaining the trust of stakeholders. Developing AI techniques that are fair, transparent and robust has been identified as a viable way of enhancing confidence in AI. However, there is an added layer of challenge for this effort moving forward. Societies are increasingly concerned about data privacy and user confidentiality. With stricter laws, such as the General Data Protection Regulation (GDPR), the existing centralized AI training paradigm must be revised to meet regulatory compliance.

Federated Learning (FL), a learning paradigm that enables collaborative training of machine learning models in which data reside in data silos and are not shared during the training process, can help AI thrive in the privacy-focused regulatory environment. As FL allows self-interested data owners to train machine learning models collaboratively, end-users can become co-creators of AI solutions. Currently, FL requires a central trusted entity to coordinate co-creators. However, in practice, such a trusted entity is hard to find and can become a single point of failure. In addition, the assumption that all co-creators receive the same final FL model regardless of their contributions introduces unfairness and limits the adoption of FL. Trustworthy federated learning is a promising and desirable direction for the field to enable open collaboration among FL co-creators and enhance the adoption of FL. It aims to support communities of data owners to self-organize during FL model training based on trust through transparency, fairness and robustness, without exposing sensitive local data. In this special issue, we aim to publish the latest advances in trustworthy federated learning to stimulate interdisciplinary thinking and promote developments that can help steer this field towards an even more socially responsible trajectory.

Scope of the Special Issue

This special issue aims to provide a timely collection of research updates to benefit researchers and practitioners working in trustworthy federated learning systems. Topics of interest include but are not limited to:

- Auditable Federated Learning
- Byzantine and Backdoor Attacks in Federated Learning
- Client Selection in Federated Learning
- Data Poisoning Attacks in Federated Learning
- Data Reconstruction Attacks in Federated Learning
- Data Selection in Federated Learning
- Decentralized Federated Learning
- Eavesdropping in Federated Learning Networking
- Fairness-Aware Federated Learning
- Feature Selection in Federated Learning
- Federated Learning for Non-IID Data
- Federated Learning with Blockchain
- Heterogeneity-Aware Federated Learning

- Incentive Mechanisms in Federated Learning Systems
- Interpretability in Federated Learning
- Large-Scale Federated Learning
- Membership Inference Attacks in Federated Learning
- Model Extraction Attacks in Federated Learning
- Model Inversion Attacks in Federated Learning
- Model Poisoning Attacks in Federated Learning
- Privacy Preserving Techniques for Federated Learning
- Property Inference Attacks in Federated Learning
- Provable Security for Federated Learning
- Robustness Aggregation for Federated Learning
- Social Responsibility in Federated Learning Systems
- Transferable Federated Learning
- Verifiable Federated Learning
- Vertical Federated Learning

Timeline:

- Submissions deadline: June 01, 2023
- Notification of the first review: August 01, 2023
- Submission of revised manuscript: October 01, 2023
- Notification of final decision: December 01, 2023

Guest Editors:

- Qiang Yang, Hong Kong University of Science and Technology
- Han Yu, Nanyang Technological University, Singapore
- Sin G. Teo, Agency for Science, Technology and Research, Singapore
- Bo Li, University of Illinois Urbana-Champaign, USA
- Guodong Long, University of Sydney, Australia
- Chao Jin, Agency for Science, Technology and Research, Singapore
- Lixin Fan, WeBank, China
- Yang Liu, Tsinghua University, China
- Le Zhang, University of Electronic Science and Technology of China

Submission Instructions

- Read the Information for Authors at http://cis.ieee.org/tnnls
- Submit your manuscript at the TNNLS webpage (http://mc.manuscriptcentral.com/tnnls) and follow the submission procedure. Include the following instructions in the header of the first page of your manuscript and cover letter: “Please submit the manuscript to the Special Issue on Trustworthy Federated Learning