Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Federated Learning for Internet of Things and Big Data

CALL FOR PAPERS

Federated learning (FL) is a feasible solution to solve the problems of data islands, break data barriers, and protect data security and privacy, especially in the context of the Internet of Things (IoT), and big data. Distributed IoT and big data users need to collaboratively train a classification or regression model to implement perfect data prediction results without compromising privacy. Unlike privacy-preserving outsourced training, rather than submitting data to the centralized cloud server, users train data locally in FL. The federated center is only responsible for aggregating the gradient information (or model parameters) uploaded by users and distributing the global training model.

Although FL can create collaborative training over heterogeneous sourced data, there are still many technical problems and privacy challenges, such as communication efficiency, system heterogeneity, data heterogeneity, computational efficiency and accuracy, data privacy, and malicious attacks. Malicious adversaries in the FL scenario of IoT and big data, or an untrusted federated center, can reversely deduce the original data and tags based on gradient information. Therefore, before data uploading, the gradient needs to be encrypted or disinfected. Moreover, communication efficiency is the information bottleneck of federated learning in IoT and big data. To alleviate the communication quality problem in IoT and big data, reducing the number of communication rounds or the message size of each round will be considered. Additionally, system heterogeneity and statistical heterogeneity are also important aspects. The development of FL should enhance the robustness against unreliable and dropout users and develop feasible strategies such as heterogeneous data alignment and fusion based on meta-learning. Attack methods in machine learning are also applicable to FL; how to detect and avoid model updating attacks. Moreover, data poison attack is also an important research area.

The aim of this Special Issue is to solicit original research articles, highlighting the developments, and security challenges for federated learning in IoT, and big data. Review articles discussing the state of the art are also welcome.

Potential topics include but are not limited to the following:

- FL training framework in IoT, big data, and multimedia communications
- High effectiveness and efficiency FL framework in IoT, and big data
- Asynchronous and heterogenetic FL training models in IoT, and big data
- Privacy-preserving FL training framework in IoT, and big data
- Meta-learning method for FL framework in IoT, and big data
- Homomorphic encryption for FL training in IoT, and big data
- Secure multiparty computing for FL training in IoT, and big data
- Differential privacy for FL training in IoT, and big data
- Lightweight, secure and producible FL framework in IoT, and big data
- Applicable conditions for privacy-preserving federated transfer learning
- FL encryption, alignment, and fusion of heterogeneous big data
- Termination conditions for FL training over heterogeneous data, and big data
- Attacks and defenses for FL framework in IoT, and big data
- Actual federated composite application framework in IoT, and big data
- Incentive mechanism design, comprehensive evaluation service system, and blockchain for FL framework in IoT, and big data

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=661279.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Jinbo Xiong, Fujian Normal University, Fuzhou, China
jbxiong@fjnu.edu.cn

Guest Editors
Lei Chen, Georgia Southern University, Statesboro, USA
lchen@georgiasouthern.edu

Narasimha Shashidhar, Sam Houston State University, Houston, USA
karpoor@shsu.edu

Zuobin Ying, Nanyang Technological University, Singapore
james.ying@ntu.edu.sg

Submission Deadline
Friday, 23 April 2021

Publication Date
September 2021