

## Call for Papers

### Recent Advances on Federated Learning in Mobile Edge Computing and Internet of Things

Federated learning (FL) is a feasible solution to solve the problems of data islands and break data barriers and protect data security and privacy. Distributed mobile edge computing (MEC) and Internet of Things (IoT) users collaborate to train a classification or regression model. Unlike privacy-preserving outsourced training, in federal learning, rather than submitting data to the centralized cloud server, users train data locally. The federated center is only responsible for aggregating the gradient information (or model parameters) uploaded by users and distributing the global training model. Although federated learning can realize collaborative training over heterogeneous sourced data, there are still many technical problems and privacy challenges, such as communication efficiency, system heterogeneity, data heterogeneity, data privacy and malicious attacks.

In a federated learning scenario, malicious adversaries in a public MEC, IoT, or an untrusted federated center can easily reversely deduce the original data and tags based on gradient information. Therefore, before uploading, the gradient needs to be encrypted or disinfected via methods such as homomorphic encryption, secure multi-party computing, differential privacy, sparse methods, etc. Moreover, communication efficiency is the information bottleneck of federated learning in MEC and IoT. In order to alleviate the communication quality problem of MEC and IoT, reducing the number of communication rounds or the message size of each round will be considered, such as using gradient quantization and other methods. Additionally, system heterogeneity and statistical heterogeneity are also important aspects. The development of federated learning 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 federated learning; therefore, how to detect and avoid model updating attacks and data poisons attacks is also an important research direction.

The journal invites submissions for a special issue on “**Recent Advances on Federated Learning in Mobile Edge Computing and Internet of Things**” that aims to attract high-quality papers that describe state-of-the-art technologies and new findings for federated learning in MEC and IoT.

Some of the most important areas include, but are not limited to:

- Efficient and robust federal training framework in MEC and IoT
- Extreme and asynchronous communication schemes for federated learning
- Privacy-preserving federal training framework in MEC and IoT
- Encryption alignment and fusion of heterogeneous data in IoT
- Termination conditions for federal training over heterogeneous data
- Fine-grained privacy constraints with executable environment
- Weakly-supervised and unsupervised federal learning
- Meta-learning method for federated learning in MEC and IoT
- Applicable conditions for privacy-preserving federated transfer learning
- Attacks and Defenses for federated learning in MEC and IoT
- Actual federated composite application framework in MEC and IoT
- Comprehensive evaluation service system for federated learning
- Lightweight, secure and producible federal learning in MEC and IoT
- Incentive mechanism design in federated learning in MEC and IoT
- Blockchain and federated learning in MEC and IoT
- Blockchain and federated learning in mobile crowdsensing
- Federated Learning in mobile multimedia communications
- Security, trust and privacy challenges in mobile multimedia communications, MEC and IoT

Successfully deploying multimedia services and applications in mobile environments requires adopting an interdisciplinary approach where multimedia, networking and physical layer issues are addressed jointly. Content

features analysis and coding, media access control, multimedia flow and error control, cross-layer optimization, Quality of Experience (QoE), media cloud as well as mobility management and security protocols are research challenges that need to be carefully examined when designing new mobile media architectures. We also need to put a great effort in designing applications that take into account the way the user perceives the overall quality of the provided service. Within this scope, MOBIMEDIA is intended to provide a unique international forum for researchers from industry and academia, working on multimedia coding, mobile communications and networking fields, to study new technologies, applications and standards. Original unpublished contributions are solicited that can improve the knowledge and practice in the integrated design of efficient technologies and the relevant provision of advanced mobile multimedia applications.

MOBIMEDIA 2021 is organized by European Alliance for Innovation (EAI). It is the world's leading and most comprehensive conference focused on artificial intelligence, mobile computing and Internet of Things.

This Special Issue is dedicated on Federated Learning in MEC and IoT. The key target audience will be the best papers accepted for the MOBIMEDIA 2021 (Guiyang, China, July 23-25, 2021). An open call for papers in this area is also included.

It is expected that submissions will address the topic of the conference and contain at least 50% new content regarding conference paper. Authors are encouraged to submit high-quality, original work that has neither appeared in, nor is under consideration by, other journals.

Please submit your paper to [Manuscript Central](#) as the "Recent Advances on FL in MEC and IoT" special issue. Submissions should be prepared for publication according to the journal [submission guidelines](#).

**Important Dates:**

Manuscript submission deadline: September 01, 2021

Expected acceptance deadline: January 01, 2022

Expected publication date: March, 2022

**Guest Editors:**

**Jinbo Xiong**

Fujian Normal University, China

[jbxiong@fjnu.edu.cn](mailto:jbxiong@fjnu.edu.cn)

**Lei Chen**

Georgia Southern University, USA

[LChen@georgiasouthern.edu](mailto:LChen@georgiasouthern.edu)

**Narasimha Shashidhar**

Sam Houston State University,

[USAkarpoor@shsu.edu](mailto:USAkarpoor@shsu.edu)

**Jianbing Ni**

Queen's University, Canada

[jianbing.ni@queensu.ca](mailto:jianbing.ni@queensu.ca)

**Zuobin Ying**

Nanyang Technological University, Singapore

[james.ying@ntu.edu.sg](mailto:james.ying@ntu.edu.sg)