Special Session Proposal for CloudCom 2025

Title: Secure and efficient distributed machine learning in cloud computing

Organizers:

Xuehe Wang, Sun Yat-sen University, wangxuehe@mail.sysu.edu.cn

Zhe Wang, Nanjing University of Science and Technology, zwang@njust.edu.cn

Yiyang, Pei, Singapore Institute of Technology, yiyang.pei@singaporetech.edu.sg

Xiao Zhang, Department of Computer Science, South-Central Minzu University, e-mail: xiao.zhang@my.cityu.edu.hk

Abstract:

With the exponential growth of data generated by cloud-based services and edge devices, distributed machine learning has become a foundational pillar of modern AI applications. In particular, decentralized learning schemes—such as federated learning—have emerged as promising solutions that facilitate collaborative model training across multiple clients without requiring the exchange of raw data. This paradigm is particularly well-suited to cloud computing environments, where stringent privacy regulations, heterogeneous network conditions, and limited communication bandwidth pose significant challenges. Nonetheless, achieving robust security and maintaining high system efficiency in such distributed settings remain critical and unresolved issues.

Cloud infrastructures, despite offering substantial computational capabilities, are inherently characterized by resource asymmetry, dynamic connectivity, and diverse privacy constraints. Conventional distributed training frameworks, originally designed for centralized data centers with homogeneous hardware and stable networking, often prove inadequate in these heterogeneous and privacy-sensitive scenarios. Moreover, the distributed nature of decentralized learning introduces unique challenges, including Non-IID data distributions, client unreliability, asynchronous updates, and susceptibility to adversarial behaviors.

This special session aims to explore the convergence of secure and efficient distributed machine learning with cloud computing. We welcome original research contributions, forward-looking position papers, and preliminary investigations that address the theoretical foundations, algorithmic innovations, and practical deployments of secure, scalable, and efficient learning frameworks in distributed cloud environments. Topics of interest include, but are not limited to:

Topics of Interest:

•Optimization Techniques for Distributed Learning in the Cloud (e.g., beyond first-order methods, adaptive and asynchronous optimization)

• Communication- and Resource-Efficient Distributed Learning (e.g., communication compression, update sparsification, hardware co-design)

• Handling System and Statistical Heterogeneity (e.g., data, model, and device heterogeneity; personalization strategies; cross-device and cross-silo settings)

• Privacy-Preserving and Secure Learning Protocols (e.g., differential privacy, secure aggregation, robustness to adversarial attacks)

• Incentive Mechanisms and Economic Models (e.g., game-theoretic designs, reputation systems, auctions, pricing)

• Foundation Models in Federated/Distributed Contexts (e.g., parameter-efficient fine-tuning, knowledge distillation)

• Responsible and Trustworthy Learning (e.g., fairness, bias, interpretability, accountability, ethical considerations)

• Domain-Specific Applications (e.g., secure medical collaboration, financial forecasting with sensitive data, smart city and IoT analytics)

Format and Duration:

[Specify the format (e.g., paper presentations, keynotes, panels) and the expected duration (half-day or full-day).]

This special session is planned as a half-day event and will feature oral paper presentations.

Expected Number of Submissions:

30-50

Previous Editions:

None.

Program Committee (Tentative):

• Zhiguang Cao, School of Computing and Information Systems, Singapore Management University, Singapore

• Wenya Wang, College of Computing and Data Science, Nanyang Technological University, Singapore

• Chuan Chen, School of Computer Science and Engineering, Sun Yat-sen University, China

• Pan Lai, Department of Computer Science, South-Central Minzu University, China

• Wenhao Yuan, School of Artificial Intelligence, Sun Yat-sen University, China

Important Dates:

• Paper Submission: September 6, 2025

• Notification of Acceptance: October 4, 2025

• Camera-Ready: October 30, 2025

• Special Session Date: November 13, 2025 (TBC)

Contact:

For any questions regarding this proposal, please contact:

wangxuehe@mail.sysu.edu.cn