



CALL FOR PAPERS



IMPORTANT DATES

15 November 2023 Special Session & Workshop Proposals Deadline 15 December 2023 Competition & Tutorial Proposals Deadline 15 January 2024

Paper Submission Deadline **15 March 2024** Paper Acceptance Notification

1 May 2024 Final Paper Subm

Final Paper Submission & Early Registration Deadline **30 June - 5 July 2024**

IEEE WCCI 2024 Yokohama, Japan

ORGANIZERS

A/Prof Guodong Long

University of Technology Sydney Guodong.long@uts.edu.au

A/Prof Zenglin Xu

Harbin Institute of Technology, Shenzhen

and Peng Cheng Lab, China

xuzenglin@hit.edu.cn

A/Prof Jing Jiang

University of Technology Sydney jing.jiang@uts.edu.au

Yue Tan

University of Technology Sydney <u>yue.tan@student.uts.edu.au</u>

A/Prof Han Yu

School of Computer Science and Engineering, Nanyang Technological University, Singapore han.yu@ntu.edu.sg

Prof Irwin King

The Chinese University of Hong Kong, Hong Kong

Trustworthy Federated Learning: in the Era of Foundation Models

IJCNN 2024 The International Joint Conference on Neural Networks (IJCNN) covers a wide range of topics in the field of neural networks, from biological neural networks to artificial neural computation.

Special Session Abstract

Federated Learning (FL) is an emerging machine learning paradigm that allows multiple endusers to collaboratively train models without sharing their private data. Existing FL frameworks are undergoing a significant change fueled by Foundation Models (FM), which presents a unique opportunity to unlock new possibilities, challenges, and applications in AI research. A robust, trustworthy FL platform can be established by examining the interplay between FL and FM, allowing them to benifit each other mutually. Also, it is necessary to overcome potential challenges incurred by original heterogeneity issues, high communication and computations costs, and privacy and security issues in FL.

This special session on trustworthy FL aims to explore recent advances in the intersection of the FM and FL, inspiring future research that can enhance both fields and propel the development of trustworthy AI systems. The session welcomes contributions on all aspects of trustworthy FL, with a special focus on its intersection with foundation model.

Topics of Interest

- Algorithmic Advances, Novel Issues, and Open Challenges in FL
- Theoretical Analysis for Trustworthy FL
- Advancing Trustworthy FL for FM
- Robustness and Reliability for Trustworthy FL
- Improving FM with Decentralized Data
- Heterogeneity in FL and FM
- Fairness of FL and FM
- Interpretability and Explainability of FL and FM
- Personalized FL based on FM
- FL Trust Policy and Strategies
- Performance Evaluation Methods, Metrics of FL Systems
- Tools and Resources (e.g., Benchmark Datasets, Software Libraries, ...)
- Security and Privacy of FL for FM (e.g., Differential Privacy, Adversarial Attacks, etc.)
- Applications of FL (e.g., Healthcare, Edge Devices, Advertising, Social Networks, etc.)