

INVITED TALK

TRUSTWORTHY FEDERATED LEARNING:
TOOLBOXES, BENCHMARKS, AND MODELS

PROFESSOR ZENGLIN XU

- Distinguished Professor at the AI Innovation and AI³ Incubation Institute at Fudan University
- AI Scientist with the Shanghai Academy of AI for Science
- Vice President of the International Neural Network Society (INNS) and the Chair of the INNS Section on AI for Education

Short Bio

Prof. Zenglin Xu received his Ph.D. in Computer Science and Engineering from The Chinese University of Hong Kong. He was previously affiliated with Purdue University, Saarland University, Max Planck Institute for Informatics, Michigan State University, UESTC, and Harbin Institute of Technology, Shenzhen. His research interests include trustworthy machine learning, federated learning, foundation models, tensor networks, and AI for Science. He has authored over 200 papers in leading AI venues. He serves as Vice President of INNS, Founding Editor-in-Chief of Academia AI and Applications, and is regularly recognized among the Stanford/Elsevier Top 2% Most-Cited Scientists.



Visit our research group pages for more.

Abstract

This talk explores trustworthy federated learning for privacy-sensitive data distributed across devices and organizations. It presents privacy-preserving methods, toolboxes such as FedLab and F4LLM, benchmarks such as FedLegal and FedCVD, and representative federated models. It also outlines a taxonomy spanning explainability, fairness, robustness, and privacy-security, and concludes with open research challenges for federated learning in the foundation-model era.

Key Highlights

Federated Learning

Privacy Preservation

Trustworthy AI

Foundation Models

Date:
October 19, 2026Time:
10 - 11 AMOrganizers:
Prof. Francesco Piccialli, Prof. Salvatore
Cuomo, Prof. Marco Lapegna, Prof. Valeria
Mele and Dr. Fabio GiampaoloLocation:
**Sala Conferenze e del Consiglio
Dipartimento di Matematica e Applicazioni "R. Caccioppoli" - I Livello**