Xiyuan Yang

Phone: (+86) 139 9819 6766 | **E-mail:** yangxiyuan@whu.edu.cn | **Homepage:** xiyuanyang45.github.io

EDUCATION

Wuhan University, Wuhan, China Sept 2021 - June 2025 (Expected)
Bachelor of Computer Science

- **Average score:** 89.2/100.0, **GPA:** 3.77/4.00 (WES GPA: 3.84/4.00)
- **Research area:** Trustworthy Machine Learning **(**Federated Learning, Differential Privacy), Large Language Models
- **Core courses:** *Higher Mathematics, Linear algebra, C Language Programming, Data Structure, Probability and Statistics, Discrete mathematics, Operating Systems, Database Systems, Principle of Computer Organization, Computer Architecture, Computer Networks*
- **Honor's program:** Outstanding Engineer Class (Elite Class) Sept 2021 - June 2025

PUBLICATION

[1] Xiyuan Yang, Shengyuan Hu, Tian Li. "Differentially Private Federated Clustering with Random Rebalancing". (First Author)
[2] Xiyuan Yang, Wenke Huang, Mang Ye. "FedAS: Bridging Inconsistency in Personalized Federated Learning". Accepted by **CVPR 2024**. (First Author)
[3] Xiyuan Yang, Wenke Huang, Mang Ye. "Dynamic Personalized Federated Learning with Adaptive Differential Privacy". Accepted by **NeurIPS 2023**. (Co-first Author)
[4] Xiuwen Fang, Mang Ye, **Xiyuan Yang**. "Robust Heterogeneous Federated Learning under Data Corruption". Accepted by **ICCV 2023**. (Third Author)

RESEARCH EXPERIENCE

Research Intern at **Microsoft Research Asia**, Social Computing Group Beijing, China
Supervised by Principal Researcher Fangzhao Wu July 2024 - Now

- **[Ongoing]** Designed a universal LLM defense method against jailbreak prompts utilizing the generalization limitations of adversarial jailbreak attacks.

Research Intern at **University of Chicago** Remote
Supervised by Prof. Tian Li Feb 2024 - Sept 2024

- **[1]** Proposed a light-weighted and effective add-on with random rebalancing technique, which can be directly applied on existing federated clustering algorithms and improve the privacy/utility tradeoffs significantly.

Research Student at **Wuhan University**, MARS Group Wuhan, China
Supervised by Prof. Mang Ye Sept 2022 - Jan 2024

- **[2]** Designed a client-level synchronization and model-level alignment to mitigate the inherent inconsistency in personalized federated learning, finally contributing better model personalization.
- **[3]** Proposed a dynamic personalized federated learning method by identifying critical parameters and keeping them from noise distortion of DP, achieving better privacy-utility trade-off while keeping privacy.
- **[4]** Introduced a corruption-robust augmentation training method and heterogeneous model distillation in federated learning, addressing the critical problem of both data heterogeneity and model heterogeneity.

SERVICE & ACTIVITY

Reviewer of Top Conf: CVPR and SCI Q1 Journals: Inf Fusion, IEEE TKDE, CAAI TRIT 2024
IEEE Student Member 2023 - 2024
Vice Minister of the Technology Department, Microsoft Student Club of WHU 2022 - 2024

SCHOLARSHIP

Overseas exchange and study scholarship of Wuhan Univeristy (Top 5%) 2024
LeiJun Computer Research Funding Scholarship (Top 0.5%) 2024

COMPETITION

MIND News Recommendation Competition (Rank 1/112 groups) May 2024

- Incorporated pretrained LMs as the news encoder and user encoder, and achieved SOTA performance.

PROJECT EXPERIENCE

Chatbot Design Based on LLaMA-33B June 2023

- Fine-tuned the pre-trained LLaMA model on open-source Chinese corpus to improve its ability in Chinese conversations.
- Used QLoRA technology to greatly reduce Video Memory usage, enabling fine-tuning on a single 3090.

CPU Design for RISC-V Instruction Set (Course Project) Mar 2023

- Used the Verilog language to design and implement a five-stage pipeline CPU, including IF/ID/EX/MEM/WB stages.
- Implemented the decoding and execution of the RISC-V instruction set, including arithmetic, logic, load/store, branch, etc.

SKILLS

Technical: Proficient in Python, PyTorch and other related tools for deep learning and data analysis, Skilled in C/C++; Familiar with Java, common front-end technologies, Haskell functional programming language, and MySQL database