Wenhan Wu

+86-150-5609-2891 | wenhanwu@whu.edu.cn | wuwenhan564@gmail.com

Wuhan, Hubei - 430072, P.R.China

Education

- **Master: Wuhan University** *2023.09 - now*
  Major in Computer Science and Technology Wuhan, China
  - Weighted Grade: 94.45/100.00 (rank 1st/187)

- **Bachelor: Wuhan University** *2019.09 - 2023.06*
  Major in Computer Science and Technology Wuhan, China
  - Weighted Grade: 91.25/100.00

Publications

C=Conference, J=Journal, S=In Submission, T=Thesis, *=Co-first Author

[C.1] Wenhan Wu, Jiawei Jiang, and Chuang Hu. **Aegis: Post-Training Attribute Unlearning in Federated Recommender Systems against Attribute Inference Attacks**. In Proceedings of the ACM Web Conference 2025 (WWW' 25), April 28–May 2, 2025, Sydney, NSW, Australia. ACM, New York, NY, USA, 11 pages. DOI: 10.1145/3696410.3714823.

[C.2] Wenhan Wu, Yili Gong, Jiawei Jiang, Chuang Hu, Xiaobo Zhou and Dazhao Cheng. **Defending against Attribute Inference Attacks in Post-Training of Recommendation Systems via Unlearning**. In IEEE International Conference on Data Engineering 2025 (ICDE' 25), May 19–23, 2025, Hong Kong SAR, China. IEEE, New York, NY, USA, 14 pages. DOI: 10.1109/ICDE65448.2025.00200.

[C.3] Wenhan Wu, Huanghuang Liang, Yingling Yuan, Jiawei Jiang, Kanye Ye Wang, Chuang Hu, Xiaobo Zhou and Dazhao Cheng. **Zero-shot Federated Unlearning via Transforming from Data-Dependent to Personalized Model-Centric**. In the 34th International Joint Conference on Artificial Intelligence (IJCAI' 25), August 16–22, 2025, Montreal, QC, Canada. IJCAI, California, USA, 9 page. DOI: 10.24963/ijcai.2025/733.

[J.1] Wenhan Wu, Huanghuang Liang, Tianyu Tu, Jiawei Jiang, Dazhao Cheng and Chuang Hu. **Mimir: Data-free Federated Unlearning through Client-Specific Prompt Generation for Personalized Models**. IEEE Transactions on Mobile Computing (TMC' 25). DOI: 10.1109/tmc.2025.3570018.

[J.2] Yukun Xu*, Wenhan Wu*, Yili Gong, Ye Wang, Chuang Hu, and Dazhao Cheng. **Frustum: Achieving High Throughput in Blockchain Systems through Hierarchical and Pipelined Sharding**. Blockchain 2024(1):0002. DOI: 10.55092/blockchain20240002.

[S.1] Wenhan Wu, Zheyuan Liu, Chongyang Gao, Ren Wang and Kaize Ding. **Beyond Sharp Minima: Robust LLM Unlearning via Feedback-Guided Multi-Point Optimization**. International Conference on Learning Representations (ICLR' 26), *Summitted*. Arxiv/2509.20230.

[S.2] Wenhan Wu, Zhili He, Huanghuang Liang, Yili Gong, Jiawei Jiang, Chuang Hu and Dazhao Cheng. **REMISVFU: Vertical Federated Unlearning via Representation Misdirection for Intermediate Output Feature**. The 40th Annual AAAI Conference on Artificial Intelligence (AAAI' 26), *Under Phase 2 Review*.

[S.3] Rui Lu*, Wenhan Wu*, Shiping Si, Chuang Hu and Dan Wang. **A Privacy-preserving Real-time Video Analytics System via Policy-based Image Transformation**. ACM Transactions on Internet Technology (TOIT' 25), *Under Review*.

[T.1] Wenhan Wu. **Performance Anomaly Detection and Bottleneck Diagnosis Mechanisms in the Android System**. Bachelor's thesis, Wuhan University (*Excellent Bachelor's Thesis Award*).

Academic Project Experiences

- **Robust Unlearning for Large Language Models against Relearning Attacks (Summer Intern).** *2025.05 - 2025.09*
  - **Problem:** LLMs excel at processing vast information but face challenges in privacy and data forgetting. When handling "forget requests", models must thoroughly forget specific data while resisting "relearning attacks" that attempt to recover forgotten information.
  - **Methods:** Employed bi-level feedback-guided optimization combined with adversarial parameter perturbations to train models to resist relearning and jailbreaking attacks during the unlearning process.
  - **Results:** Ongoing research with Northwestern University and the University of Notre Dame. Submitted to ICLR.

- **Attribute Unlearning in Federated/Non-Federated Recommendation Systems.** *2024.04 - 2024.12*

- **Problem:** Addressing privacy vulnerabilities in user embeddings exposed to attribute inference attacks, potentially induced by malicious clients or users via intentional attribute exposure.
- **Methods:** Developing a post-training mutual information-based unlearning framework that enables flexible attribute indistinguishability without requiring model retraining. To balance privacy preservation with system performance, a parameter self-sharing mechanism can further be applied for dual-objective optimization.
- **Results:** The related work has been accepted by WWW' 25 and ICDE' 25.

- **Client-Level Federated Unlearning in a Zero-Shot Manner.** *2023.05 - 2024.06*
  - **Problem:** In FL, a client may wish to exit after the model training is completed. This exit request often arises due to privacy changes after training, meaning that the client's data may no longer be available. A zero-shot client unlearning mechanism is required in such cases.
  - **Methods:** Embedding the client's personalized knowledge into the model, and achieving data-free zero-shot unlearning by forgetting the target client's specialized knowledge via knowledge distillation.
  - **Results:** The related work has been accepted by IJCAI' 25 and TMC' 25.

- **Additional Experiences.**
  - My research experiences extend to federated learning fairness analysis, blockchain-based decentralized architectures, and edge computing optimizations via TVM compiler-driven operator tuning for mobile deep learning deployments.

Industrial Project Experiences

- **Reinforcement Learning-Based Frequency Adjustment and Its Generalization in Mobile Devices.** *2024.11 - 2025.09*
  OPPO Inc.
  - **Problem:** Balancing the power and performance of the front applications via RL in heterogeneous mobile systems.
  - **Methods:** Proposing using DQN-based RL for frequency adjustment in heterogeneous CPU clusters. Employing a transfer learning approach to achieve rapid online adaptation to different foreground applications (Ongoing...).

- **Performance Anomaly Detection and Bottleneck Diagnosis in the Android System.** *2022.11 - 2023.09*
  OPPO Inc.
  - **Problem:** Addressing system performance anomalies while front-end application jank in the Android system.
  - **Methods:** Proposing a decision tree-based detection mechanism combined with bottleneck hyperplane repair diagnostics to solve memory/CPU/GPU anomalies caused by background applications.
  - **Results:** The project was successfully closed, and an Invention Patent application (202310756598.6) is in progress.

Honors and Awards

- **Honors and Scholarships.**
  - Open-source Contribution (OSPP 2025): Federated fine-tuning for LLMs in Huawei's KubeEdge-Ianvs project.
  - Chinese National Scholarship, Pacemaker to Merit Student(<0.5%), First-Class Graduate Scholarship, Didi Inc. Scholarship, National Encouragement Scholarship, Excellent Graduate Student, Excellent Thesis Award, etc.

- **Competition Achievement.**
  including but not limited to
  - National 2nd Prize in the "Huawei Cup" China Post-graduate Mathematical Contest in Modeling.
  - National 3rd Prize in China College Service Outsourcing Innovation and Entrepreneurship Competition (5/289).
  - National 2rd Prize in the Chinese Mathematics Competitions, etc.

Teaching and Academic Services

- **Teaching Assistant Service.**
  - Software Engineering course TA in the Hongyi Class (Honors Program) for undergraduate students at Wuhan University, with an Excellent Teaching Assistant Award.

- **Academic Service.**
  - TMC and AAAI Reviewer. Assisted in reviewing TPDS, WWW, IJCAI, ICDCS, ICA3PP, ICCCN, DSE, etc.

Skills

- **Skills.**
  - **Programming Languages**: Python, C/C++, Java, HTML/CSS, SQL Tools, LaTeX.
  - **Frameworks**: PyTorch, Tensorflow, SSM, Git.