CURRICULUM VITAE

Zikai Zhang（张子凯）

1664 N. Virginia Street, Reno, NV 89557, USA
Email: zikaiz@unr.edu, zikaizhang@ieee.org,
Google Scholar

EDUCATION

Jan. 2023-Present **Department of Computer Science & Engineering, University of Nevada, Reno, USA**
Ph.D. in Computer Science and Engineering

Sep. 2018-Jun. 2021 **Department of Computer Science and Technology, Huaqiao University, China**
M.Eng. in Computer Technology

Sep. 2014-Jul. 2018 **Department of Mechatronics & Vehicle Engineering, East China Jiaotong University, China**
B.Eng. in Mechanical Manufacturing and Automation

PREPRINTS

[1] **Zikai Zhang**, Rui Hu, Ping Liu, and Jiahao Xu. *"Fed-pilot: Optimizing LoRA Allocation for Efficient Federated Fine-Tuning with Heterogeneous Clients."* Under Review.

[2] **Zikai Zhang**, Rui Hu, and Jiahao Xu. *"Heterogeneous Federated Fine-Tuning with Parallel One-Rank Adaptation."* Under Review.

[3] **Zikai Zhang**, Rui Hu, and Jiahao Xu. *"SelfGrader: Detecting Jailbreak Attacks on Large Language Models with Token-Level Logit Distribution."* Under Review.

SELECTED PUBLICATIONS

[1] Yan Gao, Massimo Roberto Scamarcia, Javier Fernandez-Marques, Mohammad Naseri, Chong Shen Ng, Dimitris Stripelis, Zexi Li, Tao Shen, Jiamu Bai, Daoyuan Chen, **Zikai Zhang**, Rui Hu, InSeo Song, Lee KangYoon, Hong Jia, Ting Dang, Junyan Wang, Zheyuan Liu, Daniel Janes Beutel, Lingjuan Lyu, and Nicholas D Lane. *"FlowerTune: A Cross-Domain Benchmark for Federated Fine-Tuning of Large Language Models."* Advances in Neural Information Processing Systems, NeurIPS (2025). (Core A*, CCF-A)

[2] Jiaohao Xu, **Zikai Zhang**, Rui Hu. *"On the Out-of-Distribution Backdoor Attack for Federated Learning."* The 26th International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, ACM MobiHoc (2025). (Core A, CCF-B)

[3] **Zikai Zhang**, Suman Rath, Jiaohao Xu, and Tingsong Xiao. *"Federated Learning for Smart Grid: A Survey on Applications and Potential Vulnerabilities."* ACM Transactions on Cyber-Physical Systems, ACM TCPS (2025). (IF 3.65, CCF-C)

[4] **Zikai Zhang**, Ping Liu, Jiahao Xu, and Rui Hu. *"Fed-HeLLo: Efficient Federated Foundation Model Fine-Tuning with Heterogeneous LoRA Allocation."* IEEE Transactions on Neural Networks and Learning Systems, TNNLS (2025). (JCR-Q1, IF 8.9, CCF-B)

[5] Jiahao Xu, **Zikai Zhang**, and Rui Hu. *"Detecting Backdoor Attacks in Federated Learning via Direction Alignment Inspection."* Proceedings of the Computer Vision and Pattern Recognition Conference, CVPR (2025). (Core A*, CCF-A)

[6] Jiahao Xu, **Zikai Zhang**, and Rui Hu. *"Achieving Byzantine-Resilient Federated Learning via Layer-Adaptive Sparsified Model Aggregation."*, IEEE/CVF Winter Conference on Applications of Computer Vision ,WACV (2025). (Core A)

[7] **Zikai Zhang**, and Rui Hu. *"Byzantine-robust Federated Learning with Variance Reduction and Differential Privacy."* 2023 IEEE Conference on Communications and Network Security, IEEE CNS (2023). (IEEE ComSoc Core Conference)

[8] Zichen Liang, Hu Cao, Chu Yang, **Zikai Zhang**, Guang Chen. *"Global-local Feature Aggregation for Event-based Object Detection on Eventkitti."* 2022 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, IEEE MFI (2022). (IEEE RAS Important Conference)

[9] Siyuan Cheng, Binfei Chu, Bineng Zhong, **Zikai Zhang**, Xin Liu, ZhenJun Tang, and XianXian Li. *"DRNet: Towards Fast, Accurate and Practical Dish Recognition."* Science China-Technological Sciences (2021). (JCR-Q1, CCF-A)

[10] **Zikai Zhang**, Bineng Zhong, Shengping Zhang, Zhenjun Tang, Xin Liu, and Zhaoxiang Zhang. *"Distractor-Aware Fast Tracking via Dynamic Convolutions and MOT Philosophy."* Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, CVPR (2021). (Core A*, CCF-A)

ACADEMIC EXPERIENCE

Jan. 2023-Present **Department of Computer Science & Engineering, University of Nevada, Reno, USA**
Graduate Research/Teaching Assistant, Advisor: Dr. Rui (Zoey) Hu

Sep. 2022-Nov. 2022 **Institute of Perceptual Interaction, Nanchang Virtual Reality Research Co., Ltd, China**
Algorithm Engineer

Aug. 2021-Mar. 2022 **Institute of Intelligent Vehicle, Tongji University, China**
Research Assistant

Apr. 2021-Jul. 2021 **Department of Research, DMAI, Inc., Guangzhou, China**
Research Intern

Apr. 2018-Jun. 2021 **Computer Vision and Pattern Recognition Lab, Department of Computer Science and Technology, Huaqiao University, China**
Advisor: Dr. Bineng Zhong
M.Eng Thesis: Deep Convolutional Neural Network based Long-term Object Tracking and Object Detection

TEACHING/MENTORING EXPERIENCE

2025 Fall **Graduate Teaching Assistant,** CS442/642 Cloud Computing, **UNR, Reno, Nevada, USA.**

2025 Spring **Graduate Teaching Assistant,** CS302 Data Structure, **UNR, Reno, Nevada, USA.**

2023-2024 **Graduate Mentor,** Capstone Project for Undergraduates, **UNR, Reno, Nevada, USA.**

- ➢ Students List: Cody Long, Zachary Strazi, Kristian Konstantinov, Jacob Ayers
- ➢ Automatic Speech Recognition Attack with Adversarial Examples

2023 Summer **Graduate Mentor,** Research Experiences for Undergraduates (REU), **UNR, Reno, Nevada, USA.**

- ➢ Students List: Manny Ortiz (Penn State University), Zhang Lin (Colorado School of Mines)
- ➢ Backdoor Attack in Federated Learning System
- ➢ Supported by NSF #2150394

2019-2020 **Sessional Lecturer,** Web Interaction Design **for Undergraduates in Software Engineering Department, Xiamen Institute of Technology, Xiamen, Fujian, China.**

- ➢ Introduction of JavaScript; JavaScript Objects and Arrays; Introduction of jQuery; jQuery Selector; jQuery DOM Object; jQuery Elements and Sets; jQuery Events and Animation; jQuery Function; Validation Engine and Regular Expression.

SCHOLARSHIP AND GRANT

Aug. 2025 **HDRFS Student Publication & Travel Support,** NSF EPSCoR, USA, 1,500 USD.

2024-2025 **Co-PI, Nevada WateReuse Research Grant,** WateReuse Association, USA, 2,500 USD.

Oct. 2023 **2023 IEEE CNS Travel Grant,** NSF, USA, 1,200 USD.

2018-2021: **Graduate Innovation Fund** in Scientific Research, Huaqiao University, China, ~2,800 USD.

CONFERENCE AND COMPETITIONS

Dec. 2023 **Invited Talker,** Computational Modeling and Analysis Core Meet at UNR, Online

Oct. 2023 **First Place Poster,** 2023 UNR CyberSecurity Conference, Reno, NV, USA

Oct. 2023 **Oral,** IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA.

Nov. 2022 **Exhibitor,** 2022 World VR Industry & Metaverse Exhibition, Nanchang, China.

July. 2021 **Poster Presenter**, IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2021), Online.

May-Aug. 2020 **TOP 1% (22/2245), Silver Medal**, **Kaggle Global Wheat Detection Competition**, Computer Vision Problems in Plant Phenotyping (CVPPP) Workshop, 2020 European Conference on Computer Vision (ECCV), Online.

Jul.-Oct. 2020 **TOP 1% (5/489)**, **Electric Vehicle Helmet Recognition Competition**, The 3rd Chinese Conference on Pattern Recognition and Computer Vision (PRCV2020), Nanjing, China.

PATENT

[1] Zhong, B., **Zhang, Z**., Zheng, Y., Liang, Q., Li, X. (2021.10). *"Wheat Head Detection Method based on Computer Vision Semi-supervised Pseudo Label Learning."* CN PATENT (CN113554627A)

[2] Zhong, B., **Zhang, Z.**, Zheng, Y., Tang, Z., Li, X., Liu, X. (2021.7). *"Low-power Consumption Real-time Helmet Detection Method based on Computer Vision Target Detection."* CN PATENT (CN113128476A).

ACADEMIC SERVICE

Reviewer for:

[Journals]

IEEE Transactions on Neural Networks and Learning Systems

IEEE/ACM Transactions on Networking

Information Processing and Management

IEEE Open Journal of the Communications Society

China Communication

Journal of Information Security and Applications

IEEE Latin America Transactions

[Conferences]

The International Conference on Learning Representations (ICLR) 2026

International Conference on Machine Learning (ICML) 2025

Conference on Neural Information Processing Systems (NeurIPS) 2024, 2025

Conference on Neural Information Processing Systems (NeurIPS) Datasets and Benchmarks 2022

IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2025

International Conference on Computer Vision (ICCV) 2025

IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) 2025

International Conference on Pattern Recognition (ICPR) 2025

IEEE Consumer Communications & Networking Conference (CCNC) 2024, 2025

IEEE International Conference on Computer Communications and Networks (ICCCN), 2025

PC Board for:

PC Member, The 39th Annual AAAI Conference on Artificial Intelligence (AAAI) 2025

TPC Member, International Conference on Smart Mechatronics (ICSMech) 2024

TPC Member, International Conference on Intelligent Knowledge Systems and Engineering Applications (IKSEA) 2024

Reviewer Board, MDPI Electronics 2024-present

Reviewer Board, SciencePG Mathematics and Computer Science (MCS) 2022-present