Chenqing Zhu

Ph.D. Student, Southeast University
Research Interests: LLM Security, Multimodal LLM Security, Federated Learning, Backdoor Attacks, AI Safety Evaluation
Email: chenqingzhu@seu.edu.cn / chenqing_zhu@outlook.com
Homepage: https://chenqing-zhu.github.io

EDUCATION

Southeast University - Ph.D. Student Jiangsu, China
Duration: 09/2024-Present
Major: Cyberspace Security (Artificial Intelligence Track)
Supervisor: Prof. Songze Li

Hong Kong University of Science and Technology (Guangzhou)– Master Guangdong, China
Duration: 09/2022-06/2024
Major: Internet of Things, Supervisor: Prof. Songze Li and Prof. Danny Hin Kwok TSANG

Soochow University - Bachelor Jiangsu, China
Duration: 09/2018-06/2022
Major: Software Engineering (GPA: 3.9/4.0, Ranking: 1/79)

SELECTED PUBLICATIONS

[1] **C. Zhu,** Y. Dai, Y. Tian, Q. Li, and S. Li, "When the Aggregator Cheats: Data-Free Backdoors in Federated LLM-based QA Systems," in Proceedings of the 35th USENIX Security Symposium, 2026. Accepted.

[2] **C. Zhu** and S. Li, "Client-Driven Federated Learning under Dynamic Mixtures of Distributions," in Proceedings of the 21st International Conference on Wireless Algorithms, Systems, and Applications (WASA), 2026. Accepted.

[3] J. Xie, **C. Zhu,** and S. Li, "FedMeS: Personalized Federated Continual Learning Leveraging Local Memory," Federated Learning Workshop at IJCAI, 2023; arXiv preprint arXiv:2404.12710, 2024.

RESEARCH EXPERIENCE

Data-Free Backdoors in Federated LLM-based QA Systems
Research Project | Southeast University | 2024–2026

- Proposed a data-free server-side backdoor attack against federated LLM-based QA systems, where a malicious aggregator implants advertisement-style backdoors without accessing client raw data.
- Developed a gradient-inversion-based pipeline to reconstruct domain-relevant semantic cues and synthesize poisoned pseudo-QA data for deployment-time backdoor injection.
- Evaluated the attack across medical, mental health, and legal QA scenarios under multiple LLMs, Full FT/LoRA settings; **accepted by USENIX Security 2026.**

Client-Driven Federated Learning under Dynamic Mixtures of Distributions
Research Project | HKUST(GZ) / Southeast University| 2023–2026

- Proposed a client-driven federated learning framework for dynamic mixtures of client distributions with

asynchronous client-initiated model updates.

- Designed a server-side cluster repository to support personalized model adaptation under changing client data distributions.
- Evaluated the method on rotated FashionMNIST, CIFAR-100, MiniImageNet-100, and digit-domain benchmarks; **accepted by WASA 2026.**

FedMeS: Personalized Federated Continual Learning

Collaborative Research Project | HKUST(GZ) | 2022–2024

- Collaborated on FedMeS, a personalized federated continual learning framework that leverages local memory to mitigate client drift and catastrophic forgetting.
- Contributed to algorithm design and theoretical analysis, including memory-assisted gradient calibration during training and personalized inference with local-memory-based KNN Gaussian modeling.
- Evaluated the method across continual federated benchmarks with varying datasets, task distributions, and client numbers; accepted by FL-IJCAI'23 and released as an arXiv preprint.

Industry Collaboration

OmniTrust: Enterprise LLM Safety and Data Security Evaluation

Project Organizer / Client-facing Lead | Southeast University | 2025–Present

- Helped build **OmniTrust,** an enterprise-oriented LLM safety evaluation framework for assessing data security, compliance risks, and unsafe model behaviors in real-world deployment scenarios.
- Organized and led project execution, including evaluation scope definition, test case design, client communication, task coordination, and assessment report delivery.
- Designed evaluation dimensions covering privacy leakage, enterprise-sensitive information exposure, prompt injection, harmful outputs, data boundary violations, and China AI regulatory compliance; led a case study for a multinational chemical company in China.

INTERNSHIPS

Back-end Development Intern @ ByteDance Hangzhou 03/2022-08/2022

- Worked on Linux kernel and virtualization-related backend testing.
- Studied mainstream testing and development frameworks for Linux kernel and CPU/GPU virtualization.
- Participated in the development of FAST, an automated health-status check system for backend network servers.

Azure Network Support Engineer Intern @ Microsoft Wuxi 07/2021-09/2021

- Worked on Azure networking, including virtual networks, load balancers, VPN, and IaaS network connectivity.
- Assisted in troubleshooting customer-side network connectivity and performance issues.
- Gained experience in interactions between on-premise devices and cloud computing centers.

Teaching EXPERIENCE

Teaching Assistant: AI Security and Privacy, Southeast University 03/2025-06/2025

- Assisted in organizing a seminar-style course on AI security and privacy.
- Supported course logistics, project organization, and student evaluation.
- Covered topics related to trustworthy AI, privacy, security, and LLM safety.

TECHNICAL SKILLS

Programming & Deep Learning

- Python, PyTorch, Hugging Face Transformers, experiment automation
- Java, SQL, GoLang, etc.

Systems & Tools

- Linux, Git, Docker, LaTeX

AI Security & LLMs

- LLM fine-tuning, LoRA/PEFT, federated LLM training, gradient inversion, backdoor attacks, prompt injection evaluation

Languages

- Chinese: Native
- English: Professional working proficiency
- TOEFL: 105
- GRE: 324 + 3.5