Miao Lin

Ph.D. Student · Department of Computer Science

Old Dominion University, 5115 Hampton Blvd, Norfolk, VA 23529

✉ mlin020@odu.edu

Education

Old Dominion University	*Norfolk, US*
PhD, Department of Computer Science	*08/2023 - Present*
Central South University	*Changsha, China*
Master of Medicine	*08/2020 - 06/2023*
Hunan University of Medicine	*Huaihua, China*
Bachelor of Science	*08/2016 - 06/2020*

Teaching & Outreach

05/2025 – 10/2025 **Entrepreneur Lead**, *NSF Regional I-Corps Program*. Conducted 40+ customer-discovery interviews on privacy-tech needs; refined problem–solution fit, value proposition, and go-to-market strategy for a cybersecurity startup concept.

09/2025 - 10/2025 **Guest Lecturer**, *CYSE635 (AI Security & Privacy)*, School of Cybersecurity, ODU. Taught core concepts of cybersecurity defense, including common software vulnerabilities, attack vectors, and mitigation best practices. Conducted hands-on lab sessions using SEED Labs, working with real-world malware and exploits to reinforce defensive techniques.

07/2024 - 05/2025 **Curriculum Co-designer**, *CYSE635/CS695 (AI Security & Privacy)*, School of Cybersecurity, ODU. Redesigned course curriculum to incorporate emerging threats against LLMs; created hands-on laboratory exercises with virtual environments; integrated current research findings and industry best practices; established assessment metrics aligned with industry certifications.

05/2024 - 08/2024 **Curriculum Developer**, *NSF T3-CIDERS CyberTraining Program*. Developed and delivered cybersecurity training workshops for high school teachers. Emphasized foundational security concepts and cybersecurity awareness at the K–12 education level, bridging academic knowledge and practical classroom application.

07/2023 – 12/2024 **Teaching Assistant**, *CS 467/567: Introduction to Reverse Software Engineering*, Department of Computer Science, ODU. Led labs and grading; supported lectures on static/dynamic analysis, Win x86/64, API hooking, DLL/process injection, and network analysis; mentored an AI-assisted malware-analysis capstone.

Research Experience

Trustworthy AI

My current research secures AI models for edge devices by advancing defense mechanisms against emerging adversarial and data-poisoning/backdoor threats. Over the past two years, I identified a critical vulnerability and, leveraging this insight, designed a novel defense with rigorous theoretical analysis. The approach shows promise for real-world applications such as voice assistants and facial recognition, and I am now refining and expanding the algorithm to improve robustness and adaptability across broader deployments.

Publications

M. Lin, F. Yu, R. Ning, L. Li, Q. Lou, M. Zheng, C. Xin, H. Wu. RPP: a certified poisoned-sample detection framework for backdoor attacks under dataset imbalance. Under review in *International Conference on Learning Representations* (ICLR), 2026.

M. Lin, J. Zhang, J. Li, F. Yu, L. Li, C. Xin, H. Wu, R. Ning. ACS-Boot: efficient randomized smoothing for robustness certification on resource-constrained edge devices. Under review in *IEEE Conference on Computer Communications*(INFOCOM), 2026.

Z. Chen, J. Li, **M. Lin**, A. Mao, L. Li, R. Ning, C. Xin, H. Wu. TrojanEdge: mutual information–enhanced robust and persistent backdoor attacks for edge and on-device deployments. Under review in *IEEE Conference on Computer Communications* (INFOCOM), 2026.

M. Lin, D. Xiong, D. Lang, *et al.* SLCO4A1-mediated transmembrane transport of lysionotin attenuates acute lung injury by activating the AMPK/Nrf2 signaling pathway. *Phytotherapy Research*. 2025: 39.10: 4404-4427.

L. Deng, W. Xie, **M. Lin**, *et al.* Taraxerone inhibits M1 polarization and alleviates sepsis-induced acute lung injury by activating SIRT1. *Chinese Medicine*. 2024; 19:159.

W. Xie, L. Deng, **M. Lin**, *et al.* Sirtuin 1 mediates the protective effects of echinacoside against sepsis-induced acute lung injury by regulating the NOX4–Nrf2 axis. *Antioxidants*. 2023; 12(11):1925.

M. Lin, W. Xie, D. Xiong, *et al.* Cyasterone ameliorates sepsis-related acute lung injury via AKT(Ser473)/GSK3β(Ser9)/Nrf2 pathway. *Chinese Medicine*. 2023; 18:136.

Awards & Honors

- **2024-2025 Dominion Scholar, ODU** *2024*
- **Provincial Excellent Undergraduate** *2020*
- **Second Prize Scholarship, CSU** *2020, 2021, 2022*
- **National Scholarship, CSU** *2019*