

Shang Ma

✉ sma5@nd.edu 📞 +1 574 339 9811 🏠 Homepage **in** LinkedIn 🐙 GitHub 🎓 Scholar

Research Directions

My research focuses on building **structured AI to understand and defend against cyber fraud**. I ground AI in graphs, code semantics, and human psychology to analyze digital threats and support safer interactions for people and AI agents. My work spans two connected directions:

- **App and AI Agent Security:** Ad fraud detection [7]; UI agents for software testing [2, 5]; UI agent security [3].
- **Online Scam Understanding and Defense:** Psychological understanding [4, 6]; real-time detection [1]; timely intervention [4].

Professional Experience

NEC Laboratories America

Research Intern – Integrated Systems

Mentor: Biplob Debnath

Princeton, NJ

Jun. 2026 – Aug. 2026

- Research on memory for proactive LLM agents. Developed ProMem, a hierarchical memory framework with intent-aware retrieval for timely intent detection and context-aware task execution.

Research Intern – Data Science & System Security

Mentor: Wei Cheng

Jan. 2026 – Apr. 2026

- Research on AI-generated image detection. Formulated detection as one-class out-of-distribution learning with information bottleneck regularization to suppress spurious generator-specific features.

Charm Security

Research Collaborator

Remote

Jun. 2025 – Present

- Agentic AI to prevent and resolve scams and fraud in real time banking.

Asian Institute of Digital Finance, NUS

Research Assistant

Singapore

Oct. 2024 – Jan. 2025

- Characterizing and detecting banking scams, specifically analyzing the psychological techniques and social engineering tactics used by fraudsters.

Feysh Tech

Research Intern

Shanghai, China

Mar. 2023 – Dec. 2023

- LLM-assisted static problem analysis for automated program repair.

Publications

* Equal contribution. Full publication list: Google Scholar.

- [1] W. Sun*, **S. Ma***, Y. Li, T. Ma, Z. Wang, C. Nelson, X. Xiao, Y. Ye. PreScam: A Benchmark for Predicting Scam Progression from Early Conversations. *Conference on Language Modeling (COLM)*, 2026.
- [2] **S. Ma**, X. Xiao, Y. Ye. Agent+P: Guiding UI Agents via Symbolic Planning. *AACL Main Conference*, 2026.
- [3] C. Chen, Z. Zhang, B. Guo, **S. Ma**, I. Khalilov, S. A. Gebreegziabher, et al. The Obvious Invisible Threat: Vulnerabilities of LLM-Powered GUI Agents to Adversarial UI Manipulations in Web Interaction Tasks. *ACM Transactions on AI Security and Privacy (TAISAP)*, 2026.
- [4] **S. Ma**, C. Yanai, A. Ben, Z. Liu, Y. Ye, X. Xiao. The Anatomy of Scam Scenarios: Large-Scale Characterization and Conversation-Aware Detection. *arXiv:2606.16052*, 2026.
- [5] **S. Ma**, W. Cheng, Y. Ye, X. Xiao. From UI to Code: Mobile Ads Detection via LLM-Unified Static-Dynamic Analysis. *arXiv:2604.03561*, 2026.
- [6] **S. Ma**, T. Ma, J. Liu, W. Song, Z. Liang, X. Xiao, Y. Ye. PsyScam: A Benchmark for Psychological Techniques in Real-World Scams. *Findings of EMNLP*, 2025.
- [7] **S. Ma***, C. Chen*, S. Yang, S. Hou, T. J.-J. Li, X. Xiao, T. Xie, Y. Ye. Careful About What App Promotion Ads Recommend! Detecting and Explaining Malware Promotion via App Promotion Graph. *Network and Distributed System Security (NDSS) Symposium*, 2025.
- [8] Z. Ouyang, C. Zhang, S. Hou, **S. Ma**, C. Chen, T. Li, X. Xiao, C. Zhang, Y. Ye. Symbolic Prompt Tuning Completes the App Promotion Graph. *ECML PKDD*, 2024.

- [9] B. Li, **S. Ma**, R. Deng, K.-K. R. Choo, J. Yang. Federated Anomaly Detection on System Logs for the Internet of Things: A Customizable and Communication-Efficient Approach. *IEEE Transactions on Network and Service Management*, 19(2):1705–1716, 2022.
- [10] B. Li, P. Wang, H. Huang, **S. Ma**, Y. Jiang. FIPhish: Reputation-based Phishing Byzantine Defense in Ensemble Federated Learning. *IEEE Symposium on Computers and Communications (ISCC)*, 2021. Best Paper Award.

Education

University of Notre Dame

Ph.D. in Computer Science and Engineering

*Notre Dame, IN
Sept. 2022 – May 2027 (expected)*

- Advisor: Yanfang (Fanny) Ye. Co-advised by Xusheng Xiao at Arizona State University.

Sichuan University

B.Eng. in Cybersecurity

*Chengdu, China
Sept. 2018 – Jun. 2022*

- Wuyuzhang Honors College. GPA: 3.88/4.0.

Service

- **Conference / Workshop Reviewer:** ICLR 2026; CCS 2026 Demo; HAIPS@COLM.
- **Journal Reviewer:** Software Testing, Verification and Reliability; ACM Transactions on the Web.
- **Teaching Assistant:** Theory of Computing (CSE-30151-01), University of Notre Dame, Fall 2025.
- **Research Mentor:** Notre Dame Summer Undergraduate Research.