

Shihao Weng

✉ shweng@smail.nju.edu.cn

🌐 Homepage

🐙 GitHub

🎓 Google Scholar



Education

- Present 📖 **Visiting Ph.D. Student**, Singapore Management University, Singapore.
Advisor: Prof. Xiaofei Xie.
- 2024.09 – Present 📖 **Ph.D. in Software Engineering**, Nanjing University, China.
Advisor: Prof. Yang Feng.
- 2022.09 – 2024.06 📖 **M.S. in Software Engineering**, Nanjing University, China.
- 2018.09 – 2022.06 📖 **B.E. in Computer Science and Technology**, Jiangnan University, China.

Research Publications

- 1 **Shihao Weng**, Yang Feng, Xiaofei Xie, and Jiongchi Yu. “AgentAntibody: An Adaptive Immune System for Defending LLM Agents against Prompt Injection.” In: arXiv Preprint (arXiv: 2608.04053, 2026).
- 2 **Shihao Weng**, Yang Feng, and Xiaofei Xie. “Beyond Accuracy: Policy Invariance as a Reliability Test for LLM Safety Judges.” In: arXiv Preprint (arXiv: 2605.06161, 2026).
- 3 **Shihao Weng**, Yang Feng, Jinrui Zhang, Xiaofei Xie, Jiongchi Yu, and Jia Liu. “ARGUS: Defending LLM Agents Against Context-Aware Prompt Injection.” In: arXiv Preprint (arXiv: 2605.03378, 2026).
- 4 **Shihao Weng**, Yang Feng, Jincheng Li, Yining Yin, Zhenlun Zhang, Lyuxi Liu, and Jia Liu. “TACO: Trust Assessment of Large Language Models in Coding Assistance Tasks.” In: *48th IEEE/ACM International Conference on Software Engineering (ICSE 2026)*, CCF-A.
- 5 Zhenlun Zhang, Yang Feng, **Shihao Weng**, Yining Yin, Jincheng Li, and Jia Liu. “VADA: A Multicultural Benchmark for Value-Aware Data Generation and Alignment Evaluation in LLMs.” In: *48th IEEE/ACM International Conference on Software Engineering (ICSE 2026)*, CCF-A.
- 6 **Shihao Weng**, Yang Feng, Jincheng Li, Yining Yin, Xiaofei Xie, and Jia Liu. “AtPatch: Debugging Transformers via Hot-Fixing Over-Attention.” In: *48th IEEE/ACM International Conference on Software Engineering (ICSE 2026)*, CCF-A.
- 7 **Shihao Weng**, Yang Feng, Yining Yin, Zhenlun Zhang, and Baowen Xu. “Data Preparation and Quality for Code-Centric Generative Software Engineering Tasks: A Systematic Literature Review.” In: *Frontiers of Computer Science (FCS 2025)*, CCF-B.
- 8 Yining Yin, Yang Feng, **Shihao Weng**, Xinyu Gao, Jia Liu, and Zhihong Zhao. “Lightweight Probabilistic Coverage Metrics for Efficient Testing of Deep Neural Networks.” In: *16th Asia-Pacific Symposium on Internetware (Internetware 2025)*, CCF-C.
- 9 **Shihao Weng**, Yang Feng, Yining Yin, Yuxuan Dai, Jia Liu, and Zhihong Zhao. “Seeing the Invisible: Test Prioritization for Object Detection System.” In: *Empirical Software Engineering (EMSE 2024)*, CCF-B.
- 10 Yining Yin, Yang Feng, **Shihao Weng**, Yuan Yao, Jia Liu, and Zhihong Zhao. “Dataactive: Data Fault Localization for Object Detection Systems.” In: *33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2024)*, CCF-A.

- 11 Yining Yin, Yang Feng, **Shihao Weng**, Zixi Liu, Yuan Yao, Yichi Zhang, Zhihong Zhao, and Zhenyu Chen. “Dynamic Data Fault Localization for Deep Neural Networks.” In: *The 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2023)*, CCF-A.
- 12 **Shihao Weng**, Yang Feng, Yining Yin, and Jia Liu. “Prioritizing Testing Instances to Enhance the Robustness of Object Detection Systems.” In: *14th Asia-Pacific Symposium on Internetware (Internetware 2023)*, CCF-C, **Distinguished Paper Award**.

Honors and Academic Service

Honors and Awards

- 2023–2025  **Nanjing University Outstanding Postgraduate Student Award** (three consecutive years).
- 2023  **National Scholarship for Graduate Students**, awarded by the Ministry of Education of China.
- 2021  **CCF Outstanding Undergraduate Student**, awarded by the China Computer Federation.
-  **Bronze Medal**, 45th ACM International Collegiate Programming Contest (ICPC), Asia Regional Contest.
- 2020–2021  **National Scholarship for Undergraduate Students** (two consecutive years), awarded by the Ministry of Education of China.

Academic Service

- 2026  **Reviewer**, NeurIPS 2026 Workshop (TAE).