KNOX (YUE) LIU

Ph.D. Candidate ◇ Department of Information Technology ◇ Monash University, Australia
yue.liu1@monash.edu ◇ +61 0479114068 ◇ Github ◇ Google Scholar ◇ Homepage ◇ Linkedin

SUMMARY

PhD candidate in Software Engineering at Monash University, expected to graduate in Sep 2024. Researching software security and AI alignment for software development, focusing on reliability, security, and explainability of AI-based tools, particularly large language models for code intelligence. Published 10+ papers in top-tier venues (TOSEM, CSUR, ASE, KDD, and ISSRE). Possesses strong skills in Python, machine learning, software engineering, and generative AI. Seeking roles as a Machine Learning Engineer or Applied Scientist.

EDUCATION AND CERTIFICATIONS

Ph.D. in Software Engineering, Monash University (Expected) Sep 2024
Thesis Topic: Towards Reliable LLM-based Software Development Tools
Advised by Chakkrit Tantithamthavorn, Li Li, and Chetan Arora

Bachelor of Computer Science, Southern University of Science and Technology Jun 2019
Key Courses: Artificial Intelligence, Software Engineering, Operating Systems, Machine Learning; GPA: 3.63/4.0

Visiting Ph.D. Student, Advised by David Lo at Singapore Management University Feb-Oct 2023

Microsoft Certified: Azure AI Engineer Associate 2024

AWS Certified Machine Learning – Specialty 2024-2027

TECHNICAL SKILLS

Programming: Python, Java, JavaScript
Machine Learning & AI: TensorFlow, PyTorch, Scikit-learn, NLP, LLMs (GPT, BERT), XAI, Prompt Engineering
Software Engineering: Program Analysis, Software Testing, Debugging, Git, Vulnerability Detection
Cloud & DevOps: Azure AI, AWS Machine Learning, VSCode Extension Development
Research: Statistical Analysis, Data Visualization, Empirical Analysis, Academic Writing

AWARDS AND HONORS

Monash Ph.D. Scholarship (Full Time) 2019-2024
OpenAI Researcher Access Program Funding 2024-2025
Excellent Undergraduate Thesis, Southern University of Science and Technology 2019
Chinese National Encouragement scholarship 2017-2019

RESEARCH PROJECTS

Trustworthy Machine Learning for Android Malware Detection 2020-2023
- Extensive review of ML/DL techniques for Android malware classification, revealing key industry challenges ().
- Applied explainable AI (self-attention, LIME) to uncover and mitigate biases causing unrealistic over-optimistic accuracy (99.9%) in Android malware detection, enhancing real-world applicability and trustworthiness (, ,).
- Online materials and published papers garnered 130+ GitHub stars and 100+ Google Scholar citations ().

Reliable Large Language Models for Software Engineering 2022-2024
- Developed a comprehensive taxonomy and review of large language models (LLMs) for software engineering tasks, summarizing their applications and current challenges. This work garnered 200+ Google Scholar citations (,).
- Conducted empirical studies on LLMs (T5, BERT, GPT) across various coding tasks, revealing critical issues in concept drift, dataset biases, and unreliable evaluation metrics, which often lead to over-optimistic performance evaluations (,).
- Implemented advanced techniques including model fine-tuning and SHAP for interpretability.

Enhancing AI-Generated Code Quality and Reliability 2023-2024

- Analyzed ChatGPT-generated code quality using LeetCode tasks, revealing performance decline with increasing task difficulty and program size (,).
- Identified code quality issues in AI-generated code and developed feedback prompts to enable automated self-repair.
- Research recognized by OpenAI, securing funding for further exploration of AI-generated code generation reliability.

Evaluating Security Risks in VSCode Extensions 2023-2024

- Developed an automated analysis framework to evaluate security risks in 27,000+ VSCode extensions, focusing on credential exposure and data leakage in AI-powered tools.
- Utilized program analysis, ASTs, PDGs, and NLP-based classification to identify vulnerabilities, revealing 8.5% of extensions and 54.2% of AI coding assistants potentially leak credentials.
- Reported findings to affected vendors, resulting in 20+ responses and subsequent fixes to address identified security issues.

PUBLICATIONS

Published

- Yue Liu, Chakkrit Tantithamthavorn, Yonghui Liu, and Li Li. **On the Reliability and Explainability of Language Models for Program Generation**. In *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2024, 33(5): 1-26. [pdf] [code] ***(Core A*, CCF A)***
- Yue Liu, Thanh Le-Cong, Ratnadira Widyasari, Chakkrit Tantithamthavorn, Li Li, Xuan-Bach D. Le, and David Lo. **Refining ChatGPT-Generated Code: Characterizing and Mitigating Code Quality Issues**. In *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2024, 33(5): 1-26. [pdf] [code] ***(Core A*, CCF A)***
- Yue Liu, Chakkrit Tantithamthavorn, Yonghui Liu, Patanamon Thongtanunam, and Li Li. **Automatically Recommend Code Updates: Are We There Yet?**. In *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2024, to appear. [pdf] ***(Core A*, CCF A)***
- Yue Liu, Chakkrit Tantithamthavorn, Li Li, and Yepang Liu. **Explainable AI for Android Malware Detection: Towards Understanding Why the Models Perform So Well?**. In the *33rd International Symposium on Software Reliability Engineering (ISSRE)*, IEEE, 2022: 169-180. [pdf] [code] ***(Core A, CCF B)***
- Yue Liu, Chakkrit Tantithamthavorn, Li Li, and Yepang Liu. **Deep Learning for Android Malware Defenses: a Systematic Literature Review**. In *ACM Computing Surveys (CSUR)*, 2022, 55(8): 1-36. [pdf] [code] ***(Core A*, SCI-Q1)***
- Yue Liu, Adam Ghandar, and Georgios Theodoropoulos. **Online NEAT for Credit Evaluation–a Dynamic Problem with Sequential Data**. In the *2nd KDD Workshop on Anomaly Detection in Finance*, August 2019. [pdf]
- Yue Liu, Adam Ghandar, and Georgios Theodoropoulos. **Island model genetic algorithm for feature selection in non-traditional credit risk evaluation**. In the *IEEE congress on evolutionary computation (CEC)*, pages 2771-2778, June 2019. [pdf] ***(Core B)***
- Yue Liu, Adam Ghandar, and Georgios Theodoropoulos. **A metaheuristic strategy for feature selection problems: Application to credit risk evaluation in emerging markets**. In the *2019 IEEE Conference on Computational Intelligence for Financial Engineering and Economics (CIFEr)*, pages 1-7, May 2019. [pdf]
- Haonan Hu, Yue Liu, Yanjie Zhao, Yonghui Liu, Xiaoyu Sun, Chakkrit Tantithamthavorn, and Li Li. **Detecting Temporal Inconsistency in Biased Datasets for Android Malware Detection**. In the *2023 38th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*, IEEE, 2023: 17-23. [pdf]

Under Review

- Yue Liu, Yanjie Zhao, Chakkrit Tantithamthavorn, Li Li, and David Lo. **TaintVSCode: Evaluating VSCode Extensions Security Risks Through Taint Analysis**. 2024.

- Yue Liu, Chakkrit Tantithamthavorn, and Li Li. **Protect Your Secrets: Understanding and Preventing Data Exposure in VSCode Extensions**. 2024.
- Xinyi Hou, Yanjie Zhao, Yue Liu, Zhou Yang, Kailong Wang, Li Li, Xiapu Luo, David Lo, John Grundy, and Haoyu Wang. **Large Language Models for Software Engineering: A Systematic Literature Review**. 2024. [pdf]
- Xinyu She, Yue Liu, Yanjie Zhao, Yiling He, Li Li, Chakkrit Tantithamthavorn, Zhan Qin, and Haoyu Wang. **Pitfalls in Language Models for Code Intelligence: A Taxonomy and Survey**. 2024. [pdf] [code]

PROFESSIONAL SERVICE ACTIVITIES

Reviewer:

- IEEE Transactions on Software Engineering (TSE, Core A*)
- The International World Wide Web Conference (WWW 2024, Core A*)
- The 18th Conference of the European Chapter of the Association for Computational Linguistics (EACL 2023, Core A)
- The 20th International Conference on Mining Software Repositories (MSR 2023, Core A)

Sub-Reviewer:

- International Conference on Software Engineering (ICSE)
- ACM Computing Surveys (CSUR)
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Information Forensics and Security

ADVISING

- Xinyu She (Master Student at Huazhong University of Science and Technology), Improving the reliability of large language models for code
- Haonan Hu (Bachelor Student at Southern University of Science and Technology), The impacts of API evolution on ML-based Android malware detection

TEACHING EXPERIENCE

- Teaching Assistant, FIT3077 Software Engineering: Architecture and Design, Monash University (Spring 2022)
- Teaching Assistant, FIT2099 Object oriented Design and Implementation, Monash University (Spring 2022)
- Teaching Assistant, FIT1051 Programming fundamentals in Java, Monash University (Fall 2022)
- Teaching Assistant, CS203 Data Structure and Algorithm Analysis, SUSTech (Fall 2018)
- Teaching Assistant, CS209 Computer System Design and Application, SUSTech (Spring 2018, Fall 2017)
- Teaching Assistant, CS201 Computer Organization Principle, SUSTech (Spring 2018)