

Kaixuan Li

AUMOVIO-NTU Corporate Lab
College of Computing and Data Science (CCDS)
Nanyang Technological University

Singapore
kaixuan.li@ntu.edu.sg
[kaixuanli-ecnu.github.io](https://github.com/kaixuanli-ecnu)

Research Interests

My research has evolved from **static program analysis** into **automated vulnerability reasoning**, spanning the full vulnerability lifecycle: detection, root-cause analysis, exploitation, repair, and tracking for supply-chain security. I pursue these directions through neuro-symbolic methods that integrate program analysis with large language models.

Employment

Nanyang Technological University		Singapore
2025 – present	Postdoctoral Research Fellow & Project Lead (Project C6), AUMOVIO-NTU Corporate Lab (formerly Continental-NTU)	
2023 – 2024	Research Assistant, Continental-NTU Corporate Lab	
2022 – 2023	Visiting Student, Cyber Security Lab, SCSE	
East China Normal University		Shanghai, China
2020 – 2025	Ph.D. Researcher, Software Engineering Institute	

Education

East China Normal University		Shanghai, China
2025	Doctor of Philosophy, Software Engineering Thesis: <i>Multi-Dimensional Analysis and Optimization Methods for Static Application Security Testing</i> (in Chinese) Advisor: Prof. Yixiang Chen	
2020	Bachelor of Engineering, Software Engineering	
Nanyang Technological University		Singapore
2022 – 2023	Visiting Ph.D. Student, School of Computer Science and Engineering Host: Prof. Yang Liu	

Honors and Awards

Research Quality

2024	ACM SIGSOFT Distinguished Paper Award, ACM Intl. Conference on the Foundations of Software Engineering (FSE)
2026	Young Outstanding Paper Award, Shanghai Association of Artificial Intelligence (SAAI)

Dissertation and Academic Recognition

2025	Distinguished Ph.D. Thesis, East China Normal University
2025	Distinguished Ph.D. Thesis, College of Information Technology, ECNU
2025	Outstanding Graduate of Shanghai (Postgraduate)
2025	“Outstanding Student Youth” Award, Software Engineering Institute, ECNU

2024	President Scholarship of East China Normal University (≤ 10 recipients per year)
2024	National Scholarship, Ministry of Education, China
2024	“Student Technological Excellence” Award, SEI, ECNU
2020 – 2025	Merit Student of East China Normal University (awarded every academic year)
2020	Outstanding Graduate of Shanghai (Undergraduate)

Travel and Visiting Awards

2022 – 2023	Visiting Ph.D. Student Scholarship, China Scholarship Council
2023, 2024, 2026	ACM SIGSOFT CAPS Travel Grants (FSE 2023, FSE 2024, ISSTA 2024, FSE 2026)

Other

2021	3rd Prize, 18th China Post-Graduate Mathematical Contest in Modelling
2020	3rd Prize, 17th China Post-Graduate Mathematical Contest in Modelling

Publications

[^] co-first author; ^{*} corresponding author.

Refereed Journal Articles

- [J1] Maoyi Xie, **Kaixuan Li**^{*}, Jingquan Ge, Wei Ma, Yuqiang Sun, Ziqiao Kong, Cen Zhang, Dongge Liu, Oliver Chang, and Yang Liu. “ARASH: Token-Efficient LLM-Assisted Crash Root Cause Analysis in Fuzz Driver Generation.” In: *ACM Transactions on Software Engineering and Methodology (TOSEM)*. 2026.
- [J2] Han Liu, Jian Zhang, Cen Zhang, Xiaohan Zhang, **Kaixuan Li**, Sen Chen, Shang-Wei Lin, Yixiang Chen, Xinghua Li, and Yang Liu. “DeepFWI: Identifying Bug-Sensitive Warnings with Multi-Modal Code-Warning Semantics.” In: *IEEE Transactions on Software Engineering (TSE)*. 2026.
- [J3] Lyuye Zhang, **Kaixuan Li**[^], Kairan Sun, Daoyuan Wu, Ye Liu, Haoye Tian, and Yang Liu. “ACFix: Guiding LLMs with Mined Common RBAC Practices for Context-Aware Repair of Access Control Vulnerabilities in Smart Contracts.” In: *IEEE Transactions on Software Engineering (TSE)*, vol. 51, no. 9, pp. 2512–2532. 2025. Presented at ICSE 2026 (Journal-First).
- [J4] Jingyun Zhu, **Kaixuan Li**[^], Sen Chen, Lingling Fan, Junjie Wang, and Xiaofei Xie. “A Comprehensive Study on Static Application Security Testing (SAST) Tools for Android.” In: *IEEE Transactions on Software Engineering (TSE)*. 2024.
- [J5] Han Liu, **Kaixuan Li**, and Yixiang Chen. “Survey on Trustworthiness Measurement for Artificial Intelligence Systems.” In: *Journal of Software*, vol. 34, no. 8, pp. 3774–3792. 2023. (in Chinese)

Magazine Articles

- [M1] **Kaixuan Li** and Yixiang Chen. “Hybrid Artificial Intelligence: Logic Reasoning for Large Language Models.” In: *Communications of the Chinese Association for Artificial Intelligence (CCAAI)*, vol. 14, no. 7, pp. 3–7. 2024. (in Chinese)

Refereed Conference Publications

- [C1] **Kaixuan Li**, Jian Zhang, Chong Wang, Sen Chen, Zong Cao, Min Zhang, and Yang Liu. “GadgetHunter: Region-Based Neuro-Symbolic Detection of Java Deserialization Vulnerabilities.” In: *Proceedings of the 34th ACM International Conference on the Foundations of Software Engineering (FSE)*. 2026.
- [C2] Meilin Li[^], **Kaixuan Li**[^], Zifan Xie, Shiyu Qiu, Ming Wen, Maolin Sun, and Hongyu Zhang. “Testing Static Analyzers via Semantic-Preserving Mutators Learned from Real-World Refactoring Practice.” In: *Proceedings of the 41st IEEE/ACM International Conference on Automated Software Engineering (ASE)*. 2026.

- [C3] Chengyue Liu, Zhengzi Xu, Lyuye Zhang, Jiahui Wu, **Kaixuan Li**, and Yang Liu. “Beyond Similarity Scores: Evidence-Based Third-Party Library Detection for C/C++ Binaries.” In: *Proceedings of the 35th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*. 2026.
- [C4] Zong Cao, Yuqiang Sun, Zhengzi Xu, **Kaixuan Li**, Yeqi Fu, Yiran Zhang, Ziqiao Kong, and Yang Liu. “Reframing Paths as Logic: Semantic Segmentation for Vulnerability Detection.” In: *Proceedings of the ACM International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA)*. 2026.
- [C5] Chengyue Liu, Zhengzi Xu, **Kaixuan Li**, Jiahui Wu, Sihao Qiu, Siyuan Li, Siyang Xiong, Yang Xiao, and Yang Liu. “Understanding the Limitations of C/C++ Binary Third-Party Library Detection Tools: An Empirical Study at Scale.” In: *Proceedings of the 34th ACM International Conference on the Foundations of Software Engineering (FSE)*. 2026.
- [C6] Rui Lu, Lyuye Zhang, **Kaixuan Li***, Min Zhang, and Yixiang Chen. “Minimizing Breaking Changes and Redundancy in Mitigating Technical Lag for Java Projects.” In: *Proceedings of the 48th International Conference on Software Engineering (ICSE)*. 2026.
- [C7] Kairan Sun, Zhengzi Xu, **Kaixuan Li**, Lyuye Zhang, Yebo Feng, Daoyuan Wu, and Yang Liu. “Learning from the Past: Real-World Exploit Migration for Smart Contract PoC Generation.” In: *Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. 2025.
- [C8] Kairan Sun, Zhengzi Xu, **Kaixuan Li**, Lyuye Zhang, Yuqiang Sun, Liwei Tan, and Yang Liu. “Fault-Seeker: LLM-Empowered Framework for Blockchain Transaction Fault Localization.” In: *Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. 2025.
- [C9] Lyuye Zhang, Jiahui Wu, Chengwei Liu, **Kaixuan Li**, Xiaoyu Sun, Lida Zhao, Chong Wang, and Yang Liu. “Fixing Outside the Box: Uncovering Tactics for Open-Source Security Issue Management.” In: *Proceedings of the 34th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*. 2025.
- [C10] **Kaixuan Li**, Jian Zhang, Sen Chen, Han Liu, Yang Liu, and Yixiang Chen. “PatchFinder: A Two-Phase Approach to Security Patch Tracing for Disclosed Vulnerabilities in Open-Source Software.” In: *Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*. 2024.
- [C11] **Kaixuan Li**, Yue Xue, Sen Chen, Han Liu, Kairan Sun, Ming Hu, Haijun Wang, Yang Liu, and Yixiang Chen. “Static Application Security Testing (SAST) Tools for Smart Contracts: How Far Are We?” In: *Proceedings of the 32nd ACM International Conference on the Foundations of Software Engineering (FSE)*. 2024. **ACM SIGSOFT Distinguished Paper Award**.
- [C12] Han Liu, Daoyuan Wu, Yuqiang Sun, Haijun Wang, **Kaixuan Li**, Yang Liu, and Yixiang Chen. “Using My Functions Should Follow My Checks: Understanding and Detecting Insecure OpenZeppelin Code in Smart Contracts.” In: *Proceedings of the 33rd USENIX Security Symposium*. 2024.
- [C13] **Kaixuan Li**, Han Liu, Lyuye Zhang, and Yixiang Chen. “Automatic Inspection of Static Application Security Testing (SAST) Reports via Large Language Model Reasoning.” In: *Proceedings of the 4th International Conference on AI Logic and Applications (AILA)*. 2024.
- [C14] **Kaixuan Li**[^], Sen Chen[^], Lingling Fan, Ruitao Feng, Han Liu, Chengwei Liu, Yang Liu, and Yixiang Chen. “Comparison and Evaluation on Static Application Security Testing (SAST) Tools for Java.” In: *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*. 2023. Study and benchmark highlighted at OWASP Global AppSec USA 2025.
- [C15] Kairan Sun, Zhengzi Xu, Chengwei Liu, **Kaixuan Li**, and Yang Liu. “Demystifying the Composition and Code Reuse in Solidity Smart Contracts.” In: *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*. 2023.

- [C16] Han Liu, Sen Chen, Ruitao Feng, Chengwei Liu, **Kaixuan Li**, Zhengzi Xu, Liming Nie, Yang Liu, and Yixiang Chen. “A Comprehensive Study on Quality Assurance Tools for Java.” In: *Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*. 2023.

Refereed Industry Briefings

- [B1] Zong Cao, Zhengzi Xu, Yeqi Fu, Yuqiang Sun, **Kaixuan Li**, and Yang Liu. “Let LLM Learn: When Your Static Analyzer Actually ‘Gets It’” *Black Hat USA 2025*, Las Vegas, USA, August 2025.

Preprints

- [R1] Mengyao Zhao, **Kaixuan Li**[^], Lyuye Zhang, Wenjing Dang, Chenggong Ding, Sen Chen, and Zheli Liu. “A Systematic Study on Generating Web Vulnerability Proof-of-Concepts Using Large Language Models.” *arXiv:2510.10148*, 2025.
- [R2] Wenjing Dang, **Kaixuan Li**[^], Sen Chen, Zhenwei Zhuo, Lyuye Zhang, and Zheli Liu. “Real-World Usability of Vulnerability Proof-of-Concepts: A Comprehensive Study.” *arXiv:2510.18448*, 2025.

Grants and Funded Projects

As Project Lead

- 2025 – 2028 **Hypervisor Cybersecurity Assessment** (Project C6). AUMOVIO-NTU Corporate Lab, Nanyang Technological University. 750K SGD.

As Independent Proposer

- 2026 **Reflective Cyber Reasoning**. Gemini Academic Program Award, Google Cloud. 20K USD.
- 2026 **Z.ai Cyber Security Partnership Program**. Z.ai. Model access and credits for security research.
- 2025 – 2026 **Towards Reliable Reasoning for Large Language Models**. Key Laboratory of Symbolic Computation and Knowledge Engineering of the Ministry of Education. 20K RMB.
- 2023 – 2024 **Compatibility Analysis and Assurance for Open-Source Software**. Huawei. 550K RMB.
- 2020 – 2022 **Innovative Approaches to Task Partitioning and Scheduling in Heterogeneous Embedded Systems**. Dean Fund, MoE Engineering Research Center for Hardware–Software Co-Design. 120K RMB.

As Co-Proposer

- 2022 – 2023 **Resilient Software Architecture Design and Elegant Downgrading**. Huawei. 600K RMB.
- 2021 – 2022 **Software Trustworthiness Measurement**. Huawei. 600K RMB.

Professional Service and Affiliations

Program Committee (Conference)

- USENIX Security Symposium, 2027
- Intl. Conference on Software Engineering (ICSE), 2026, 2027
- Intl. Conference on the Foundations of Software Engineering (FSE), 2026, 2027
- Intl. Conference on Software Engineering – Software Engineering in Practice (ICSE-SEIP), 2026
- ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), Student Research Competition, 2026
- Intl. Conference on Software Engineering (ICSE), Shadow PC, 2025
- ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), Artifact Evaluation, 2025

- Intl. Conference on AI Logic and Applications (AILA), 2025
- Intl. Conference on Mining Software Repositories (MSR), Junior PC, 2024

Journal Referee

- IEEE Transactions on Software Engineering (TSE) (2025 – present)
- IEEE Transactions on Dependable and Secure Computing (TDSC) (2025 – present)
- IEEE Transactions on Big Data (TBD) (2025 – present)
- Empirical Software Engineering (EMSE) (2025 – present)
- ACM Transactions on Software Engineering and Methodology (TOSEM) (2024 – present)
- Frontiers of Computer Science (FCS) (2024 – present)
- Cybersecurity (2023 – present)

Co-Reviewing

- ICSE 2024, 2025; FSE 2024; IEEE S&P 2025; USENIX Security 2025; CCS 2024; NDSS 2024

Teaching

2026	Tutor, <i>SC2006 Software Engineering</i> (undergraduate). Four tutorial groups, with Prof. Yang Liu. Nanyang Technological University.
2021 – 2022	Teaching Assistant, <i>Hardware–Software Co-design</i> (graduate). Tutorial lecturer. East China Normal University.
2021	Teaching Assistant, <i>Optimization and Design of Intelligent Systems</i> (undergraduate). Tutorial lecturer. East China Normal University.

Patents and Technology Disclosures

Patents

- [P1] **Kaixuan Li**, Jingquan Ge, Maoyi Xie, Yang Liu, Praveen Kakkolangara, Sheikh Mahbub Habib, and Yi Wang. “Apparatus, Data Carrier, Computer Program, and Methods for Detecting and Fixing Software Vulnerabilities.” UK Patent Application No. 2522585.5, filed 23 December 2025. [Corresponds to TD1.]
- [P2] **Kaixuan Li**, Jingquan Ge, Wei Ma, Maoyi Xie, Yang Liu, Suraj Jayakumar Menon, and Brendl Markus. “Apparatus, Data Carrier, Computer Program, and Method for Repairing a Computer Program.” UK Patent Application No. 2512389.4. *Under review*. [Corresponds to TD9.]
- [P3] Maoyi Xie, Jingquan Ge, **Kaixuan Li**, Wenbing Tang, Yang Liu, Praveen Kakkolangara, and Sheikh Mahbub Habib. “Apparatus, Data Carrier, Computer Program, and Method for Testing a Fuzz Driver for Fuzz Testing Software.” UK Patent Application No. 2512857.0. *Under review*. [Corresponds to TD5.]

Technology Disclosures

- [TD1] **Kaixuan Li** et al. “ Δ Synth: Synthesizing Static Analysis Rules for Vulnerability Detection via Semantic Mining” (2025E05037 SG).
- [TD2] **Kaixuan Li** et al. “LogicFuzz: Coordinated LLM Agents for Next-Gen Fuzz Driver Generation” (2025E04486 SG).
- [TD3] **Kaixuan Li** et al. “Automatic Java Deserialization Vulnerability Mining and Exploitation via LLM Agents” (2025E01925 SG).
- [TD4] **Kaixuan Li** et al. “PatchSleuth: Sleuthing Patch Commits for Disclosed Vulnerabilities in Open-Source Software” (2024E01727 SG).

- [TD5] Maoyi Xie, Jingquan Ge, **Kaixuan Li** et al. “ARASH: Analysis and Repair of Crash” (2025E01753 SG).
- [TD6] **Kaixuan Li** et al. “Neuro-Symbolic Detection for C/C++ Path-Sensitive Vulnerabilities” (2026E00104 SG).
- [TD7] Jingquan Ge, **Kaixuan Li** et al. “PGFilter: A Parameter-Guided, Token-Saving Source Code Filter for LLM-Based Root Cause Analysis” (2025E05430 SG).
- [TD8] Maoyi Xie, Jingquan Ge, **Kaixuan Li** et al. “Logickaller: Automata-Driven Kernel Fuzzing for Logic Bug Detection via Learned Syscall Relations” (2026E00814 SG).
- [TD9] **Kaixuan Li**, Jingquan Ge, Wei Ma, Maoyi Xie et al. “AutoPatcher: Automatic Root-Cause-Analysis Guided Program Repair via Large Language Models” (2024E04091 SG).

Industrial Impact

Deployed Tools

- 2024 – present **PatchFinder** (cf. [C10]). Deployed internally at Scantist Pte. Ltd., Singapore, for OSS vulnerability patch tracing.
- 2025 – present **ARASH** (cf. [J1], patent [P3], TD5). Deployed at AUMOVIO; partially integrated into Google’s `oss-fuzz-gen`, used in conjunction with our LogicFuzz framework (TD2).

Vulnerability Disclosures

- 2025 – 2026 **LogicFuzz** (cf. TD2) discovered and reported **20+ zero-day vulnerabilities** in popular open-source C/C++ projects; all confirmed and fixed by upstream maintainers.

Community Resources

- 2025 – present **Static Analyzer Research Papers**. Curated, continuously updated literature index on static analysis.
- 2025 – present **Proof-of-Concept (PoC) Research Papers**. Curated literature index on vulnerability proof-of-concepts.
- 2025 – present **Hypervisor Testing: Techniques, Challenges, and Future Directions**. Curated literature index on hypervisor testing.
- 2023 – present **Java CVE Bench** (cf. [C14]). Benchmark of real-world Java CVEs for evaluating SAST tools.

Invited Talks and Presentations

- Jul. 2026 “Organizing Vulnerability Knowledge for OpenHarmony.” Huawei, Shenzhen, China.
- May 2026 “Neuro-Symbolic Vulnerability Detection and Exploitation.” East China Normal University, Shanghai, China.
- Apr. 2025 “PatchFinder: A Two-Phase Approach to Security Patch Tracing for Disclosed Vulnerabilities in Open-Source Software.” CCF Technical Committee on Formal Methods, Youth Forum.
- Dec. 2024 “Static Application Security Testing (SAST) Tools for Smart Contracts: How Far Are We?” Xi’an Jiaotong University, Xi’an, China.

Referees

Prof. Yang Liu (Postdoctoral Advisor)

College of Computing and Data Science (CCDS), Nanyang Technological University
02C-84, Block N4, 50 Nanyang Avenue, Singapore
yangliu@ntu.edu.sg

Prof. Yixiang Chen (Ph.D. Advisor)

Software Engineering Institute, East China Normal University
Room 303, Mathematics Building, 3663 North Zhongshan Road, Shanghai, China
yxchen@sei.ecnu.edu.cn

Prof. Sen Chen (Close Collaborator)

College of Cryptology and Cyber Science, Nankai University
Room 563, Building of Computer Science, Jinnan Campus, Tianjin, China
senchen@nankai.edu.cn

Prof. Ting Su (Ph.D. Thesis Committee Member & Collaborator)

Software Engineering Institute, East China Normal University
Room B1103, Science Building, 3663 North Zhongshan Road, Shanghai, China
tsu@sei.ecnu.edu.cn