XIE Xiaofei

School of Computing and Information Systems
Singapore Management University (SMU)
80 Stamford Road
Singapore 178902

Email: xfxie@smu.edu.sg
Office Phone: 87984395

Education

Master of Science, Tianjin University, China, 2018

PhD, Tianjin University, China, 2018

Bachelor of Engineering, Tianjin University, China, 2011

Academic Appointments

Assistant Professor of Computer Science, School of Computing and Information Systems, SMU, Jan 2022 - Present

Awards and Honors

Distinguished Reviewer Award (ASE 2025), ASE 2025, 2025

ACM SIGSOFT Distinguished Paper Award (ASE'25), ACM SIGSOFT, 2025

ACM SIGSOFT Distinguished Paper Award (ASE'23), ACM SIGSOFT, 2023

3rd place in Trusted Media Challenge, AI Singapore, 2022

ACM SIGSOFT Distinguished Paper Award (ISSTA'22), ACM SIGSOFT, 2022

RESEARCH

Publications

Journal Articles [Refereed]

ContrastRepair: Enhancing conversation-based automated program repair via contrastive test case pairs, by Kong, Jiaolong; Xie, Xiaofei; Cheng, Mingfei; Liu, Shangqing; Du, Xiaoning; Guo, Qi. (2025). *ACM Transactions on Software Engineering and Methodology, 34* (8), 1-31. (Published)

Beyond decision: Android malware description generation through profiling malicious behavior trajectory, by WU, Chunlian; CHEN, Sen; LI, Jiaming; CHAI, Renchao; FAN, Lingling; XIE, Xiaofei; FENG, Ruitao. (2025). *ACM Transactions on Software Engineering and Methodology, 34* (7), 1-39. https://doi.org/10.1145/3715909 (Published)

Assessing the robustness of test selection methods for deep neural networks, by HU, Qiang; GUO, Yuejun;

XIE, Xiaofei; CORDY, Maxime; MA, Wei; PAPADAKIS, Mike; MA, Lei; LE TRAON, Yves. (2025). *ACM Transactions on Software Engineering and Methodology, 34* (7), 1-26. https://doi.org/10.1145/3715693 (Published)

FedGraft: Memory-aware heterogeneous federated learning via model grafting, by LIU, Ruixuan; HU, Ming; XIA, Zeke; XIE, Xiaofei; XIA, Jun; ZHANG, Pengyu; HUANG, Yihao; CHEN, Mingsong. (2025). *IEEE Transactions on Mobile Computing, 24* (12), 1-13. https://doi.org/10.1109/TMC.2025.3591537 (Published)

Runtime backdoor detection for federated learning via representational dissimilarity analysis, by ZHANG, Xiyue; XUE, Xiaoyong; DU, Xiaoning; XIE, Xiaofei; LIU, Yang; SUN, Meng. (2025). *IEEE Transactions on Dependable and Secure Computing, 22* (5), 4607-4624. https://doi.ieeecomputersociety.org/10.1109/TDSC.2025.3550330 (Published)

Enmob: Unveil the behavior with multi-flow analysis of encrypted app traffic, by GE, Mengmeng; FENG, Ruitao; LIU, Likun; YU, Xiangzhan; VINAY, Sachidananda; XIE, Xiaofei; LIU, Yang. (2025). *Cybersecurity, 8* (1), 1-17. https://doi.org/10.1186/s42400-024-00301-0 (Published)

Diversity-oriented testing for competitive game agent via constraint-guided adversarial agent training, by MA, Xuyan; WANG, Yawen; WANG, Junjie; XIE, Xiaofei; WU, Boyu; YAN, Yiguang; LI, Shoubin; XU, Fanjiang; WANG, Qing. (2025). *IEEE Transactions on Software Engineering, 51* (1), 66-81. https://doi.org/10.1109/TSE.2024.3491193 (Published)

Demo2Test: Transfer testing of agent in competitive environment with failure demonstrations, by CHEN, Jianming; WANG, Yawen; WANG, Junjie; XIE, Xiaofei; WANG, Dandan; WANG, Qing; XU, Fanjiang. (2025). *ACM Transactions on Software Engineering and Methodology, 34* (2), 1-28. https://doi.org/10.1145/3696001 (Published)

IRHunter: Universal detection of instruction reordering vulnerabilities for enhanced concurrency in distributed and parallel systems, by XIN, Guohua; XU, Guangquan; ZHANG, Yao; WEN, Cheng; ZHANG, Cen; XIE, Xiaofei; XIONG, Neal N.; LIU, Shaoying; GAO, Pan. (2025). *IEEE Transactions on Parallel and Distributed Systems, 36* (6), 1-17. https://doi.org/10.1109/TPDS.2025.3556861 (Advance Online)

A comprehensive study on static application security testing (SAST) tools for Android, by ZHU, Jingyun; LI, Kaixuan; CHEN, Sen; FAN, Lingling; WANG, Junjie; XIE, Xiaofei. (2024). *IEEE Transactions on Software Engineering, 50* (12), 3385-3402. https://doi.org/10.1109/TSE.2024.3488041 (Published)

FlexFL: Heterogeneous federated learning via APoZ-guided flexible pruning in uncertain scenarios, by CHEN, Zekai; JIA, Chentao; HU, Ming; XIE, Xiaofei; LI, Anran; CHEN, Mingsong. (2024). *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 43* (11), 4069-4080. https://doi.org/10.1109/TCAD.2024.3444695 (Accepted)

CaBaFL: Asynchronous federated learning via hierarchical cache and feature balance, by XIA, Zeke; HU, Ming; YAN, Dengke; XIE, Xiaofei; LI, Tianlin; LI, Anran; ZHOU, Junlong; CHEN, Mingsong. (2024). *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 43* (11), 4057-4068. https://doi.org/10.1109/TCAD.2024.3446881 (Published)

FOSS: Towards fine-grained unknown class detection against the open-set attack spectrum with variable legitimate traffic, by ZHAO, Ziming; LI, Zhaoxuan; XIE, Xiaofei; YU, Jiongchi; ZHANG, Fan; ZHANG, Rui; CHEN, Binbin; LUO, Xiangyang; HU, Ming; MA, Wenrui. (2024). *IEEE/ACM Transactions on Networking, 32* (5), 1-16. https://doi.org/10.1109/TNET.2024.3413789 (Advance Online)

Reinforcement learning based online request scheduling framework for workload-adaptive edge deep learning inference, by TAN, Xinrui; LI, Hongjia; XIE, Xiaofei; GUO, Lu; ANSARI, Nirwan; HUANG, Xueqing; WANG, Liming; XU, Zhen; LIU, Yang. (2024). *IEEE Transactions on Mobile Computing, 23* (12), 1-18. https://doi.org/10.1109/TMC.2024.3429571 (Advance Online)

Neuron sensitivity guided test case selection, by HUANG, Dong; BU, Qingwen; FU, Yichao; QING, Yuhao; XIE, Xiaofei; CHEN, Junjie; CUI, Heming. (2024). *ACM Transactions on Software Engineering and Methodology, 33* (7), 1-32. https://doi.org/10.1145/3672454 (Advance Online)

Unveiling code pre-trained models: Investigating syntax and semantics capacities, by MA, Wei; LIU, Shangqing; ZHAO, Mengjie; XIE, Xiaofei; WANG, Wenhang; HU, Qiang; ZHANG, Jie; YANG, Liu. (2024). *ACM Transactions on Software Engineering and Methodology, 33* (7), 1-28. https://doi.org/10.1145/3664606 (Published)

CMD: Co-analyzed IoT malware detection and forensics via network and hardware domains, by ZHAO, Ziming; LI, Zhaoxuan; YU, Jiongchi; ZHANG, Fan; XIE, Xiaofei; XU, Haitao; CHEN, Binbin. (2024). *IEEE Transactions on Mobile Computing, 23* (5), 5589-5603. https://doi.org/10.1109/TMC.2023.3311012 (Published)

Test optimization in DNN testing: A survey, by HU, Qiang; GUO, Yuejun; XIE, Xiaofei; CORDY, Maxime; MA, Lei; PAPADAKIS, Mike; LE TRAON, Yves. (2024). *ACM Transactions on Software Engineering and Methodology, 33* (4), 1-42. https://doi.org/10.1145/3643678 (Published)

Adversarial learning for coordinate regression through k-layer penetrating representation, by JIANG, Mengxi; SUI, Yulei; LEI, Yunqi.; XIE, Xiaofei; LI, Cuihua; LIU, Yang; TSANG, Ivor W.. (2024). *IEEE Transactions on Dependable and Secure Computing, 21* (6), 1-15. https://doi.org/10.1109/TDSC.2024.3376437 (Advance Online)

Active code learning: Benchmarking sample-efficient training of code models, by HU, Qiang; GUO, Yuejun; XIE, Xiaofei; CORDY, Maxime; MA, Lei; PAPADAKIS, Mike; TRAON, Yves Le. (2024). *IEEE Transactions on Software Engineering, 50* (5), 1-17. https://doi.org/10.1109/TSE.2024.3376964 (Published)

DDoS family: A novel perspective for massive types of DDoS attacks, by ZHAO, Ziming; LI, Zhaoxuan; ZHOU, Zhihao; YU, Jiongchi; SONG, Zhuoxue; XIE, Xiaofei; ZHANG, Fan; ZHANG, Rui. (2024). *Computers and Security, 138* 1-14. https://doi.org/10.1016/j.cose.2023.103663 (Published)

KAPE: kNN-based performance testing for deep code search, by GUO, Yuejun; HU, Qiang; XIE, Xiaofei; MAXIME, Cordy; PAPADAKIS, Mike; LE TRAON, Yves. (2023). *ACM Transactions on Software Engineering and Methodology, 33* (2), 1-24. https://doi.org/10.1145/3624735 (Published)

Seed selection for testing deep neural networks, by ZHI, Yuhan; XIE, Xiaofei; SHEN, Chao; SUN, Jun; ZHANG, Xiaoyu; GUAN, Xiaohong. (2023). *ACM Transactions on Software Engineering and Methodology, 33* (1), 1-33. https://doi.org/10.1145/3607190 (Published)

LaF: Labeling-free model selection for automated deep neural network reusing, by HU, Qiang; GUO, Yuejun; XIE, Xiaofei; CORDY, Maxime; PAPADAKIS, Mike; TRAON, Yves Le. (2023). *ACM Transactions on Software Engineering and Methodology, 33* (1), 1-28. https://doi.org/10.1145/3611666 (Published)

Faire: Repairing fairness of neural networks via neuron condition synthesis, by LI, Tianlin; XIE, Xiaofei; WANG, Jian; GUO, Qing; LIU, Aishan; MA, Lei; LIU, Yang. (2023). *ACM Transactions on Software Engineering and Methodology, 33* (1), 1-24. https://doi.org/10.1145/3617168 (Published)

Automated Question Title Reformulation by Mining Modification Logs From Stack Overflow, by LIU, Ke; CHEN, Xiang; CHEN, Chunyang; XIE, Xiaofei; CUI, Zhanqi. (2023). *IEEE Transactions on Software Engineering, 49* (9), 4390-4410. https://doi.org/10.1109/TSE.2023.3292399 (Published)

Demystifying Performance Regressions in String Solvers, by ZHANG, Yao; XIE, Xiaofei; LI, Yi; LIN, Yi; CHEN, Sen; LIU, Yang; LI, Xiaohong. (2023). *IEEE Transactions on Software Engineering, 49* (3), 947-961. https://doi.org/10.1109/TSE.2022.3168373 (Published)

GraphSearchNet: Enhancing GNNs via Capturing Global Dependencies for Semantic Code Search, by LIU, Shangqing; XIE, Xiaofei; SIOW, Jjingkai; MA, Lei; MENG, Guozhu; LIU, Yang. (2023). *IEEE Transactions on Software Engineering, 49* (4), 1-16. https://doi.org/10.1109/TSE.2022.3233901 (Advance Online)

Deep learning for coverage-guided fuzzing: How far are we?, by LI, Siqi; XIE, Xiaofei; LIN, Yun; LI, Yuekang; FENG, Ruitao; LI, Xiaohong; GE, Weimin; DONG, Jin Song. (2022). *IEEE Transactions on Dependable and Secure Computing,* 1-13. https://doi.org/10.1109/TDSC.2022.3200525 (Published)

Self-checking deep neural networks for anomalies and adversaries in deployment, by XIAO, Yan; BESCHASTNIKH, Ivan; LIN, Yun; HUNDAL, Rajdeep Singh; XIE, Xiaofei; ROSENBLUM, David S.; DONG, Jin Song. (2022). *IEEE Transactions on Dependable and Secure Computing,* 1-17. https://doi.org/10.1109/TDSC.2022.3200421 (Published)

Enhancing security patch identification by capturing structures in commits, by WU, Bozhi; LIU, Shangqing; FENG, Ruitao; XIE, Xiaofei; SIOW, Jingkai; LIN, Shang-Wei. (2022). *IEEE Transactions on Dependable and Secure Computing,* 1-15. https://doi.org/10.1109/TDSC.2022.3192631 (Published)

GBGallery : A benchmark and framework for game testing, by LI, Zhuo; WU, Yuechen; MA, Lei; XIE, Xiaofei; CHEN, Yingfeng; FAN, Changjie. (2022). *Empirical Software Engineering, 27* (6), 1-27. https://doi.org/10.1007/s10664-022-10158-x (Published)

An Empirical Study on Data Distribution-Aware Test Selection for Deep Learning Enhancement, by HU, Qiang; GUO, Yuejun; CORDY, Maxime; XIE, Xiaofei; MA, Lei; PAPADAKIS, Mike; LE TRAON, Yves. (2022). *ACM Transactions on Software Engineering and Methodology, 31* (4), 78:1-78:30. (Published)

NPC: Neuron Path Coverage via Characterizing Decision Logic of Deep Neural Networks, by XIE, Xiaofei; LI, Tianlin; WANG, Jian; MA, Lei; GUO, Qing; JUEFEI-XU, Felix; LIU, Yang. (2022). *ACM Transactions on Software Engineering and Methodology, 31* (3), 1-27. (Published)

Byzantine-Resilient Decentralized Stochastic Gradient Descent, by GUO, Shangwei; ZHANG, Tianwei; YU, Han; XIE, Xiaofei; MA, Lei; XIANG, Tao; LIU, Yang. (2022). *IEEE Transactions on Circuits and Systems for Video Technology, 32* (6), 4096-4106. http://doi.org/10.1109/TCSVT.2021.3116976 (Published)

Neighborhood cooperative multiagent reinforcement learning for adaptive traffic signal control in epidemic regions, by ZHANG, Chengwei; TIAN, Yu; ZHANG, Zhibin; XUE, Wanli; XIE, Xiaofei; YANG, Tianpei; GE, Xin; CHEN, Rong. (2022). *IEEE Transactions on Intelligent Transportation Systems, 23* (12), 25157-25168. https://doi.org/10.1109/TITS.2022.3173490 (Published)

Neuron Coverage-Guided Domain Generalization, by TIAN, Chris Xing; LI, Haoliang; XIE, Xiaofei; LIU, Yang; WANG, Shiqi. (2023). *IEEE Transactions on Pattern Analysis and Machine Intelligence, 45* (1), 1-12. https://doi.org/10.1109/TPAMI.2022.3157441 (Published)

JSCSP: A Novel Policy-Based XSS Defense Mechanism for Browsers, by XU, Guangquan; XIE, Xiaofei; HUANG, Shuhan; ZHANG, Jun; PAN, Lei; LOU, Wei; LIANG, Kaitai. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (2), 862-878. (Published)

DeepRepair: Style-Guided Repairing for Deep Neural Networks in the Real-World Operational Environment, by YU, Bing; QI, Hua; QING, Guo; JUEFEI-XU, Felix; XIE, Xiaofei; MA, Lei; ZHAO, Jianjun. (2022). *IEEE Transactions on Reliability, 71* (4), 1-16. (Published)

Independent Reinforcement Learning for Weakly Cooperative Multiagent Traffic Control Problem, by ZHANG, Chengwei; JIN, Shan; XUE, Wanli; XIE, Xiaofei; CHEN, Shengyong; CHEN, Rong. (2021). *IEEE Transactions on Vehicular Technology, 70* (8), 7426-7436. https://doi.org/10.1109/TVT.2021.3090796 (Published)

Breaking Neural Reasoning Architectures With Metamorphic Relation-Based Adversarial Examples, by CHAN, Alvin; MA, Lei; JUEFEI-XU, Felix; ONG, Yew-Soon; XIE, Xiaofei; XUE, Minhui; LIU, Yang. (2022). *IEEE Transactions on Neural Networks and Learning Systems, 33* (11), 1-7. https://doi.org/10.1109/TNNLS.2021.3072166 (Published)

Understanding adversarial robustness via critical attacking route, by LI, Tianlin; LIU, Aishan; LIU, Xianglong; XU, Yitao; ZHANG, Chongzhi; XIE, Xiaofei. (2021). *Information Sciences: Informatics and Computer Science Intelligent Systems Applications, 547* 568-578. https://doi.org/10.1016/j.ins.2020.08.043 (Published)

Can we trust your explanations? Sanity checks for interpreters in Android malware analysis, by FAN, Min; WEI, Wenying; XIE, Xiaofei; LIU, Yang; GUAN, Xiaohong; LIU, Ting. (2021). *IEEE Transactions on Information Forensics and Security, 16* 838-853. https://doi.org/10.1109/TIFS.2020.3021924 (Published)

Text Backdoor Detection Using an Interpretable RNN Abstract Model, by FAN, Ming; SI, Ziliang; XIE, Xiaofei; LIU, Yang; LIU, Ting. (2021). *IEEE Transactions on Information Forensics and Security, 16* 4117-4132. https://doi.org/10.1109/TIFS.2021.3103064 (Published)

A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices, by FENG, Ruitao; CHEN, Sen; XIE, Xiaofei; MENG, Guozhu; LIN, Shang-Wei; LIU, Yang. (2021). *IEEE Transactions on Information Forensics and Security, 16* 1563-1578. (Published)

Automatic Loop Summarization via Path Dependency Analysis, by XIE, Xiaofei; CHEN, Bihuan; ZOU, Liang; LIU, Yang; LE, Wei; LI, Xiaohong. (2019). *IEEE Transactions on Software Engineering, 45* (6), 537-557. (Published)

Conference Proceedings

Rising from ashes: Generalized federated learning via dynamic parameter reset, by WU, Jiahao; HU, Ming; YANG, Yanxin; XIE, Xiaofei; CHEN, ZeKai; SONG, Chenyu; CHEN, Mingsong. (2025.0). *Proceedings of the Thirty-Ninth Annual Conference on Neural Information Processing Systems, San Diego, CA, USA, 2025 December 2-7*

, (pp. 1-27) US: (Published)

Seeing is fixing: Cross-modal reasoning with multimodal LLMs for visual software issue fixing, by HUANG, Kai; ZHANG, Jian; XIE, Xiaofei; CHEN, Chunyang. (2025.0). *Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering, Seoul, Korea, November 16-20,* (pp. 1-13) Korea: (Published)

SPEC2CODE: Mapping software specification to function-level code implementation, by WANG, Yuekun; QUAN, Lili; XIE, Xiaofei; WANG, Junjie; CHEN, Jianjun. (2025.0). *Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering, Seoul, Korea, November 16-20,* Korea: https://conf.researchr.org/details/ase-2025/ase-2025-papers/198/SPEC2CODE-Mapping-Software-Specification-to-Function-Level-Code-Implementation (Published)

Defects4C: Benchmarking large language model repair capability with C/C++ bugs, by WANG, Jian; XIE, Xiaofei; HU, Qiang; LIU, Shangqing; YU, Jiongchi; KONG, Jiaolong; LI, Yi. (2025.0). *Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering, Seoul, Korea, November 16-20,* (pp. 1-12) Korea: (Published)

Do code semantics help? A comprehensive study on execution trace-based information for code large language models, by WANG, Jian; XIE, Xiaofei; HU, Qiang; LIU, Shangqing; LI, Yi. (2025.0). *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing, Suzhou, China, November 4-9*
, (pp. 10367-10385) Suzhou: ACL. https://doi.org/10.18653/v1/2025.findings-emnlp.548 (Published)

MMLU-ProX: A multilingual benchmark for advanced large language model evaluation, by XUAN, Weihao; et. al.. (2025.0). *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing, Suzhou, China, November 4-9,* (pp. 1513-1532) Suzhou: ACL. https://aclanthology.org/2025.emnlp-main.79/ (Published)

FilterFL: Knowledge filtering-based data-free backdoor defense for federated learning, by YANG, Yanxin; HU, Ming; XIE, Xiaofei; CAO, Yue; ZHANG, Pengyu; HUANG, Yihao; CHEN, Mingsong. (2025.0). *CCS '25: Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, Taipei, Taiwan, October 13-17,* (pp. 3147-3161) New York : ACM. https://doi.org/10.1145/3719027.3744883 (Published)

Gradients as an action: Towards communication-efficient federated recommender systems via adaptive action sharing, by LU, Zhufeng; JIA, Chentao; HU, Ming; XIE, Xiaofei; CHEN, Mingsong. (2025.0). *KDD '25: Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.2, Toronto, Canada, August 3-7,* (pp. 1999-2009) Toronto ON, Canada: Association for Computing Machinery. https://doi.org/10.1145/3711896.3736987 (Published)

Towards context-aware traffic classification via time-wavelet fusion network, by ZHAO, Ziming; SONG, Zhuoxue; XIE, Xiaofei; LI, Zhaoxuan; YU, Jiongchi; ZHANG, Fan Terry; LI, Tingting. (2025.0). *KDD '25: Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.2, Toronto, Canada, August 3-7,* (pp. 2089-2100) New York: ACM. (Published)

MoDitector: Module-directed testing for autonomous driving systems, by WANG, Renzhi; CHENG, Mingfei; XIE, Xiaofei; ZHOU, Yuan; MA, Lei. (2025.0). *Proceedings of the 34th ACM SIGSOFT International Symposium on Software Testing and Analysis, Trondheim, Norway, 2025 June 25-28,* (pp. 137-158) New York: ACM. https://doi.org/10.1145/3728876 (Published)

RegTrieve: Reducing system-level regression errors for machine learning systems via retrieval-enhanced ensemble, by CAO, Junming; XIANG, Xuwen; CHENG, Mingfei; CHEN, Bihuan; WANG, Xinyan; LU, You; SHA, Chaofeng; XIE, Xiaofei; PENG, Xin. (2025.0). *Proceedings of the ACM on Software Engineering, Volume 2, Issue FSE, Trondheim, Norway, 2025 June 23-27,* (pp. 1960-1982) New York: ACM. https://doi.org/10.1145/3729358 (Published)

Demystifying memorization in LLM-based program repair via a general hypothesis testing framework, by KONG, Jiaolong; XIE, Xiaofei; LIU, Shangqing. (2025.0). *Proceedings of the ACM on Software Engineering, Volume 2, Issue FSE, Trondheim, Norway, 2025 June 23-27,* (pp. 2712-2734) New York: ACM. https://dl.acm.org/doi/10.1145/3729390 (Published)

CAShift: Benchmarking log-based cloud attack detection under normality shift, by YU, Jiongchi; XIE, Xiaofei; HU, Qiang; ZHANG, Bowen; ZHAO, Ziming; LIN, Yun; MA, Lei; FENG, Ruitao; LIAU, Frank. (2025.0). *Proceedings of the ACM on Software Engineering, Volume 2, Issue FSE, Trondheim, Norway, 2025 June 23-27,* (pp. 1687-1709) New York: ACM. https://dl.acm.org/doi/10.1145/3729346 (Published)

My model is malware to you: Transforming AI models into malware by abusing TensorFlow APIs, by ZHU, Ruofan; CHEN, Ganhao; SHEN, Wenbo; XIE, Xiaofei; CHANG, Rui. (2025.0). *Proceedings of the 2025 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 12-15*
, (pp. 486-503) Los Alamitos, CA: IEEE. https://doi.org/10.1109/SP61157.2025.00012 (Published)

Decictor: Towards evaluating the robustness of decision-making in autonomous driving systems, by CHENG, Mingfei; XIE, Xiaofei; ZHOU, Yuan; WANG, Junjie; MENG, Guozhu; YANG, Kairui. (2025.0). *Proceedings of the 2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE), Ottawa, Canada, April 26 - May 6,* (pp. 1-13) Los Alamitos, CA: IEEE. https://doi.org/10.1109/ICSE55347.2025.00114 (Published)

Scenario-driven and context-aware automated accessibility testing for Android apps, by ZHANG, Yuxin; CHEN, Sen; XIE, Xiaofei; LIU, Zibo; FAN, Lingling. (2025.0). *Proceedings of the ICSE 2025 47th International Conference on Software Engineering, Ontario, Canada, April 27 - May 3,* (pp. 2777-2789) Los Alamitos, CA: IEEE. https://doi.org/10.1109/ICSE55347.2025.00093 (Published)

Dissecting global search: A simple yet effective method to boost individual discrimination testing and repair, by QUAN, Lili; LI, Tianlin; XIE, Xiaofei; CHEN, Zhenpeng; CHEN, Sen; JIANG, Lingxiao; LI, Xiaohong. (2025.0). *Proceedings of the ICSE 2025 47th International Conference on Software Engineering, Ontario, Canada, April 27 - May 3,* (pp. 1908-1920) Los Alamitos, CA: IEEE. https://doi.org/10.1109/ICSE55347.2025.00235 (Published)

Intention is all you need: Refining your code from your intention, by GUO, Qi; XIE, Xiaofei; LIU, Shangqing; HU, Ming; LI, Xiaohong; BU, Lei. (2025.0). *Proceedings of the ICSE 2025 47th International Conference on Software Engineering, Ontario, Canada, April 27 - May 3,* (pp. 1-13) Ottawa, ON, Canada: (Published)

SpecGen: Automated generation of formal program specifications via large language models, by MA, Lezhi; LIU, Shangqing; LI, Yi; XIE, Xiaofei; BU, Lei. (2025.0). *Proceedings of the ICSE 2025 47th International Conference on Software Engineering, Ontario, Canada, April 27 - May 3,* (pp. 16-28) Los Alamitos, CA: IEEE. https://doi.org/10.1109/ICSE55347.2025.00129 (Published)

TensorJSFuzz: Effective testing of web-based deep learning frameworks via input-constraint extraction, by QUAN, Lili; XIE, Xiaofei; GUO, Qianyu; JIANG, Lingxiao; CHEN, Sen; WANG, Junjie; LI, Xiaohong. (2025.0). *WWW '25: Proceedings of the ACM on Web Conference 2025, Sydney, Australia, April 28 - May 2,* (pp. 3405-3414) New York: ACM. https://doi.org/10.1145/3696410.3714649 (Published)

Understanding individual agent importance in multi-agent system via counterfactual reasoning, by CHEN, Jianming; WANG, Yawen; WANG, Junjie; XIE, Xiaofei; HU, Jun; WANG, Qing; XU, Fanjiang. (2025.0). *Proceedings of the 39th AAAI Conference on Artificial Intelligence and Thirty-Seventh Conference on Innovative Applications of Artificial Intelligence and Fifteenth Symposium on Educational Advances in Artificial Intelligence, Philadelphia, Pennsylvania, 2025 February 25 - March 4,* (pp. 15785-15794) USA: AAAI Press. https://doi.org/10.1609/aaai.v39i15.33733 (Published)

MultiSFL: Towards accurate split federated learning via multi-model aggregation and knowledge replay, by XIA, Zeke; HU, Ming; YAN, DengKe; LIU, Ruixuan; LI, Anran; XIE, Xiaofei; CHEN, Mingsong. (2025.0). *Proceedings of the 39th AAAI Conference on Artificial Intelligence and Thirty-Seventh Conference on Innovative Applications of Artificial Intelligence and Fifteenth Symposium on Educational Advances in Artificial Intelligence, Philadelphia, Pennsylvania, 2025 February 25 - March 4,* (pp. 914-922) USA: AAAI Press. https://doi.org/10.1609/aaai.v39i1.32076 (Published)

SampDetox : Black-box backdoor defense via perturbation-based sample detoxification, by YANG, Yanxin; JIA, Chentao; YAN, Dengke; HU, Ming; LI, Tianlin; XIE, Xiaofei; WEI, Xian; CHEN, Mingsong. (2024.0). *Proceedings of 38th Annual Conference on Neural Information Processing Systems (NeurIPS 2024) : Vancouver, Canada, December 10-15,* Canada: NeurIPS. (Accepted)

Themis: Automatic and efficient deep learning system testing with strong fault detection capability, by HUANG, Dong; LI, Tsz On; XIE, Xiaofei; CUI, Heming. (2024.0). *Proceeding of the 35th International Symposium on Software Reliability Engineering, Tsukuba, Japan, 2024 October 28-31*

, New Jersey: IEEE. https://doi.org/10.48550/arXiv.2405.09314 (Published)

RATCHET: Retrieval augmented transformer for program repair, by WANG, Jian; LIU, Shangqing; XIE, Xiaofei; KAI, Siow Jingkai; LIU, Kui; LI, Yi. (2024.0). *2024 35th IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW): Tsukuba, Japan, October 28-31: Proceedings,* (pp. 427-438) Pistacataway: IEEE. https://doi.org/10.1109/ISSRE62328.2024.00048 (Published)

Detecting and explaining anomalies caused by web tamper attacks via building consistency-based normality, by Yifan Liao, Ming Xu, Yun Lin, Xiwen Teoh, Xiaofei Xie, Ruitao Feng Frank Liauw, Hongyu Zhang, Jin Song Dong. (2024.0). *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering (ASE 2024) : Sacramento CA, USA, October 27 - November 1,* (pp. 531-543) Sacramento CA, USA: Association for Computing Machinery. https://doi.org/10.1145/3691620.3695024 (Published)

An empirical study to evaluate AIGC detectors on code content, by WANG, Jian; LIU, Shangqing; XIE, Xiaofei; LI, Yi. (2024.0). *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering (ASE 2024) : Sacramento CA, USA, October 27 - November 1,* (pp. 844-856) USA: Association for Computing Machinery. https://doi.org/10.1145/3691620.3695468 (Published)

AdvSCanner : Generating adversarial smart contracts to exploit reentrancy vulnerabilities using LLM and static analysis, by WU, Yin; XIE, Xiaofei; PENG, Chenyang; LIU, Dijun; WU, Hao; FAN, Ming; LIU, Tin; WANG, Haijun. (2024.0). *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering (ASE 2024) : Sacramento CA, USA, October 27 - November 1,* (pp. 1019-1031) Sacramento CA, USA: Association for Computing Machinery. https://doi.org/10.1145/3691620.3695482 (Published)

Navigating governance paradigms: A cross-regional comparative study of generative AI governance processes & principle, by LUNA, Jose; TAN, Ivan; XIE, Xiaofei; JIANG, Lingxiao. (2024.0). *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society 7th AIES 2024 : San Jose, CA, USA, October 21-23,* (pp. 917-931) USA: AAAI Press. (Published)

How effective are they? Exploring large language model based fuzz driver generation, by ZHANG, Cen; ZHENG, Yaowen; BAI, Mingqiang; LI, Yeting; MA, Wei; XIE, Xiaofei, et al.. (2024.0). *Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, Vienna, Austria, 2024 September 16–20,* (pp. 1223-1225) New York: ACM. https://doi.org/10.1145/3650212.3680355 (Published)

Bugs in pods: Understanding bugs in container runtime systems, by YU, Jiongchi; XIE, Xiaofei; ZHANG, Ceng; CHEN, Sen, et al.. (2024.0). *Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, Vienna, Austria, 2024 September 16-20,* (pp. 1364 -1376) New York: ACM. https://doi.org/10.1145/3650212.3680366 (Published)

FT2Ra: A fine-tuning-inspired approach to retrieval-augmented code completion, by GUO, Qi; LIU, Shangqing; XIE, Xiaofei; TANG, Ze Tang, et al.. (2024.0). *Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, Vienna, Austria, 2024 September 16-20,* (pp. 313-324) New York: ACM. https://doi.org/10.1145/3650212.3652130 (Published)

Enhancing multi-agent system testing with diversity-guided exploration and adaptive critical state exploitation, by MA, Xuyan; WANG, Yawen; WANG, Junjie; XIE, Xiaofei, et al.. (2024.0). *Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, Vienna, Austria, 2024 September 16-20,* (pp. 1491 -1503) New York: ACM. https://doi.org/10.1145/3650212.3680376 (Published)

Is aggregation the only choice? Federated learning via layer-wise model recombination, by HU, Ming; YUE, Zhihao; XIE, Xiaofei; CHEN, Cheng Chen, et al.. (2024.0). *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Barcelona, Spain, 2024 August 25–29,* New York: ACM. https://doi.org/10.1145/3637528.3671722 (Published)

Enhancing code vulnerability detection via vulnerability-preserving data augmentation, by LIU, Shangqing; MA, Wei; WANG, Jian; XIE, Xiaofei; FENG, Ruitao; LIU, Yang. (2024.0). *LCTES 2024: Proceedings of the 25th ACM SIGPLAN/SIGBED International Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES ’ 24), June 24, Copenhagen,* (pp. 166-177) New York: ACM. https://doi.org/10.1145/3652032.3657564 (Published)

Exploring the potential of ChatGPT in automated code refinement: An empirical study, by QI, Guo; CAO, Junming; XIE, Xiaofei; LIU, Shangqing; LI, Xiaohong; CHEN, Bihuan; PENG, Xin. (2024.0). *ISCE '24: Proceedings of the 46th IEEE/ACM International Conference on Software Engineering, Lisbon, Portugal, April 14-20,* (pp. 1-13) New York: ACM. https://doi.org/10.1145/3597503.3623306 (Published)

Exploring the potential of ChatGPT in automated code refinement: An empirical study, by GUO, Qi; LIU, Shangqing; CAO, Junming; LI, Xiaohong; PENG, Xin; XIE, Xiaofei; CHEN, Bihuan. (2024.0). *ICSE '24: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering: Lisbon, April 14-20,* (pp. 1-13) New York: ACM. https://doi.org/10.1145/3597503.3623306 (Published)

A black-box attack on code models via representation nearest Neighbor search, by ZHANG, Jie; MA, Wei;

HU, Qiang; Liu, Shangqing; XIE, Xiaofei; LE Traon, Yves; LIU, Yang. (2023.0). *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing, Singapore, December 6-10,* (pp. 9706-9716) Texas: Association for Computational Linguistics. https://doi.org/10.18653/v1/2023.findings-emnlp.649 (Published)

DistXplore: Distribution-guided testing for evaluating and enhancing deep learning systems, by WANG, Longtian; XIE, Xiaofei; DU, Xiaoning; TIAN, Meng; GUO, Qing; YANG, Zheng; SHEN, Chao . (2023.0). *ESEC/FSE '23: Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, San Francisco, December 3-9,* (pp. 68-80) New York: ACM. https://doi.org/10.1145/3611643.3616266 (Published)

Mitigating membership inference attacks via weighted smoothing, by TAN, Minghan; XIE, Xiaofei; SUN, Jun; WANG, Tianhao. (2023.0). *ACSAC '23: Proceedings of the 39th Annual Computer Security Applications Conference, Austin, December 4,* (pp. 787-798) New York: ACM. https://doi.org/10.1145/3627106.3627189 (Published)

Generative model-based testing on decision-making policies, by ZHUO, Li; WU, Xiongfei; ZHU, Derui;CHENG, Mingfei; CHEN, Siyuan; ZHANG, Fuyuan; XIE, Xiaofei; MA, Lei; ZHAO, Jianjun . (2023.0). *2023 38th IEEE/ACM International Conference on Automated Software Engineering: Luxembourg, September 11-15: Proceedings,* (pp. 243-254) Piscataway, NJ: IEEE. https://doi.org/10.1109/ASE56229.2023.00153 (Published)

EndWatch: A practical method for detecting non-termination in real-world software, by ZHANG, Yao; XIE, Xiaofei; LI, Yi; CHEN, Sen; ZHANG, Cen; LI, Xiaohong. (2023.0). *2023 38th IEEE/ACM International Conference on Automated Software Engineering: Luxembourg, September 11-15: Proceedings,* (pp. 686-697) Piscataway, NJ: IEEE. https://doi.org/10.1109/ASE56229.2023.00061 (Published)

Decompiling x86 deep neural network executables, by LIU, Zhibo; YUAN, Yuanyuan; WANG, Shuai; XIE, Xiaofei; MA, Lei. (2023.0). *Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, 2023 August 9-11,* (pp. 1-18) Berkeley, CA: USENIX. https://www.usenix.org/system/files/sec23summer_406-liu_zhibo-prepub.pdf (Published)

Automata-guided control-flow-sensitive fuzz driver generation, by ZHANG, Cen; LI, Yuekang; ZHOU, Hao; ZHANG, Xiaohan; ZHENG, Yaowen; ZHAN, Xian; XIE, Xiaofei; LUO, Xiapu; LI, Xinghua; LIU, Yang; HABIB, Sheikh M. . (2023.0). *Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, 2023, August 9-11,* (pp. 2867-2884) Berkeley, CA: USENIX. (Published)

BehAVExplor: Behavior diversity guided testing for autonomous driving systems, by CHENG, Mingfei; ZHOU, Yuan; XIE, Xiaofei. (2023.0). *ISSTA 2023: Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis, Seattle, WA, July 17-21,* (pp. 488-500) New York: ACM. https://doi.org/10.1145/3597926.3598072 (Published)

Multi-target backdoor attacks for code pre-trained models, by LI, Yanzhou; LIU, Shangqing; CHEN, Kangjie; XIE, Xiaofei; ZHANG, Tianwei; LIU, Yang. (2023.0). *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics, Toronto, Canada, July 9-14,* (pp. 7236-7254) Ohio, USA: Association for Computational Linguistics (ACL). (Published)

Evading deepfake detectors via adversarial statistical consistency, by HOU, Yang; GUO, Qing; HUANG, Yihao; XIE, Xiaofei; MA, Lei; ZHAO, Jianjun. (2023.0). *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),* (pp. 12271-12280) Canada: IEEE. https://doi.org/10.1109/CVPR52729.2023.01181 (Published)

CodeS: Towards code model generalization under distribution shift, by HU, Qiang; GUO, Yuejun; XIE, Xiaofei; CORDY, Maxime; MA, Lei; PAPADAKIS, Mike; TRAON, Yves Le. (2023.0). *Proceedings of the 45th International Conference on Software Engineering: New Ideas and Emerging Results, Melbourne, Australia, May 14-20,* (pp. 1-6) New York: (Published)

Widget detection-based testing for industrial mobile games, by WU, Xiongfei; YE, Jiaming; CHEN, Ke, XIE, Xiaofei; HU, Yujing; HUANG, Ruochen; MA, Lei; ZHAO, Jianjun . (2023.0). *Proceedings of the 45th International Conference on Software Engineering: Software Engineering in Practice, Melbourne, Australia, May 14-20,* (pp. 173-184) Los Alamitos, CA: IEEE. https://doi.org/10.1109/ICSE-SEIP58684.2023.00021 (Published)

GameRTS: A regression testing framework for video games, by YU, Jiongchi; WU, Yuechen; XIE, Xiaofei; LE, Wei; MA, Lei; CHEN, Yingfeng; HU, Yujing: ZHANG, Fan. (2023.0). *2023 IEEE/ACM 45th International Conference on Software Engineering: Melbourne, May 14-20: Proceedings,* (pp. 1393-1404) Piscataway, NJ:

IEEE. https://doi.org/10.1109/ICSE48619.2023.00122 (Published)

ContraBERT: Enhancing code pre-trained models via contrastive learning, by LIU, Shangqing; WU, Bozhi; XIE, Xiaofei; MENG, Guozhu; LIU, Yang. . (2023.0). *Proceedings of the 45th International Conference on Software Engineering,* (pp. 2476-2487) IEEE/ACM International Conference on Software Engineering: IEEE. https://doi.org/10.1109/ICSE48619.2023.00207 (Published)

Aries: Efficient testing of deep neural networks via labeling-free accuracy estimation, by HU, Qiang; GUO, Yuejun; XIE, Xiaofei; CORDY, Maxime; MA, Lei; PAPADAKIS, Mike; LE TRAON, Yves. (2023.0). *2023 IEEE/ACM 45th International Conference on Software Engineering (ISCE), Melbourne, May 14-20: Proceedings,* (pp. 1776-1787) Piscataway, NJ: IEEE. https://doi.org/10.1109/ICSE48619.2023.00152 (Published)

Neural episodic control with state abstraction, by LI, Zhuo; ZHU, Derui; HU, Yujing; XIE, Xiaofei; MA, Lei; ZHENG, Yan; SONG, Yan; CHEN, Yingfeng; ZHAO, Jianjun. (2023.0). *Proceedings of the 11th International Conference on Learning Representations, Kigali, Rwanda, 2023 May 1-5,* (pp. 1-18) Kigali, Rwanda: ICLR. (Published)

SeqAdver: Automatic payload construction and injection in sequence-based Android adversarial attack, by ZHANG, Fei; FENG, Ruitao; XIE, Xiaofei; LI, Xiaohong; SHI, Lianshuan. (2023.0). *2023 IEEE International Conference on Data Mining Workshops, ICDMW: Shanghai, December 1-4: Proceedings,* (pp. 1342-1351) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ICDMW60847.2023.00172 (Published)

Large-scale analysis of non-termination bugs in real-world OSS projects, by SHI, Xiuhan; XIE, Xiaofei; LI, Yi; ZHANG, Yao; CHEN, Sen; LI, Xiaohong. (2022.0). *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Singapore, 2022 November 14-18,* (pp. 256-268) Singapore: ACM. http://doi.org/10.1145/3540250.3549129 (Published)

TransRepair: Context-aware program repair for compilation errors, by LI, Xueyang; LIU, Shangqing; FENG, Ruitao; MENG, Guozhu; XIE, Xiaofei; CHEN, Kai; LIU, Yang. (2022.0). *ASE '22: Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering, Rochester, MI, October 10-14,* (pp. 1-13) New York: ACM. https://doi.org/10.1145/3551349.3560422 (Published)

Towards understanding the faults of JavaScript-based deep learning systems, by QUAN, Lili; GUO, Qianyu; XIE, Xiaofei; CHEN, Sen; LI, Xiaohong; LIU, Yang. (2022.0). *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering, Oakland Center, Michigan, United States, 2022 October 10-14,* (pp. 1-13) United States: ASE. (Published)

Cross-lingual transfer learning for statistical type inference, by LI, Zhiming; XIE, Xiaofei; LI, Haoliang; XU, Zhengzi; LI, Yi; LIU, Yang. (2022.0). *Proceedings of the 31th ACM SIGSOFT International Symposium on Software Testing and Analysis, Virtual Conference, 2022 July 18-22,* (pp. 239-250) Virtual Conference: ACM. https://doi.org/10.1145/3533767.3534411 (Published)

A3GAN: Attribute-aware anonymization networks for face de-identification, by ZHAI, Liming; GUO, Qing; XIE, Xiaofei; MA, Lei; WANG, Yi Estelle; LIU, Yang. (2022.0). *MM '22: Proceedings of the 30th ACM International Conference on Multimedia, Lisbon, Portugal, October 10-14,* (pp. 5303-5313) New York: ACM. https://doi.org/10.1145/3503161.3547757 (Published)

GraphCode2Vec: Generic code embedding via lexical and program dependence analyses, by MA, Wei; ZHAO, Mengjie; SOREMEKUN, Ezekiel; HU, Qiang; ZHANG, Jie M.; PAPADAKIS, Mike; CORDY, Maxime; XIE, Xiaofei; LE TRAON, Yves. (2022.0). *Proceedings of the 2022 Mining Software Repositories Conference, Pittsburgh, United States, May 23-24,* (pp. 524-536) New York: ACM. https://doi.org/10.1145/3524842.3528456 (Published)

Learning program semantics with code representations: An empirical study, by SIOW, Jing Kai; LIU, Shangqing; XIE, Xiaofei; MENG, Guozhu; LIU, Yang. (2022.0). *Proceedings of the 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering, Honolulu, Hawaii, March 15-18,* (pp. 1-12) Honolulu, Hawaii : IEEE. http://doi.org/10.1109/SANER53432.2022.00073 (Published)

SoFi: Reflection-augmented fuzzing for JavaScript engines, by HE, Xiaoyu; XIE, Xiaofei; LI, Yuekang; SUN, Jianwen; LI, Feng; ZOU, Wei; LIU, Yang; YU, Lei; ZHOU, Jianhua; SHI, Wenchang; HUO, Wei. (2021.0). *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Conference, November 15-19,* (pp. 2229-2242) Virtual Conference: Association for Computing Machinery. (Published)

Learning to adversarially blur visual object tracking, by GUO, Qing; CHENG, Ziyi; JUEFEI-XU, Felix; MA, Lei; XIE, Xiaofei; LIU, Yang; ZHAO, Jianjun. (2021.0). *Proceedings of the IEEE/CVF International Conference on*

Computer Vision 2021, Montreal, Canada, October 10-17, (pp. 10839-10848) Virtual Conference: IEEE. (Published)

An empirical study of GUI widget detection for industrial mobile games, by YE, Jiaming; CHEN, Ke; XIE, Xiaofei; MA, Lei; HUANG, Ruochen; CHEN, Yingfeng; XUE, Yinxing; ZHAO, Jianjun. (2021.0). *Proceedings of the 29th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering: ESEC/FSE 2021, Athens, Greece, August 23-28,* (pp. 1427-1437) Athens, Greece: Association for Computing Machinery. (Published)

AVA: Adversarial Vignetting Attack against visual recognition, by TIAN, Binyu; JUEFEI-XU, Felix; GUO, Qing; XIE, Xiaofei; LI, Xiaohong; LIU, Yang. (2021.0). *Proceedings of the 30th International Joint Conference on Artificial Intelligence (IJCAI-21), Montreal, 2021 Aug 19-26 ,* (pp. 1046-1053) Virtual Conference: IJCAI. (Published)

RNNRepair: Automatic RNN Repair via model-based analysis, by XIE, Xiaofei; GUO, Wenbo; MA, Lei; LE, Wei; WANG, Jian; ZHOU, Lingjun; LIU, Yang; XING, Xinyu. (2021.0). *Proceedings of the 38th International Conference on Machine Learning 2021: Virtual, July 18-24,* (pp. 11383-11392) Virtual Only: PMLR. https://proceedings.mlr.press/v139/xie21b.html (Published)

Stealing deep reinforcement learning models for fun and profit, by CHEN, Kangjie; GUO, Shangwei; ZHANG, Tianwei; XIE, Xiaofei; LIU, Yang. (2021.0). *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, Virtual Conference, June 7-11,* (pp. 307-319) Virtual Conference: Association for Computing Machinery. (Published)

Bias field poses a threat to DNN-based X-ray recognition, by TIAN, Bingyu; GUO, Qing; JUEFEI-XU, Felix; CHAN, Wen Le; CHENG, Yupeng; LI, Xiaohong; XIE, Xiaofei; QIN, Shengchao. (2021.0). *Proceedings of the 2021 IEEE International Conference on Multimedia and Expo (ICME), Virtual Conference, July 5-9,* (pp. 1-6) Virtual Conference: IEEE Computer Society. (Published)

Automatic web testing using curiosity-driven reinforcement learning, by ZHENG, Yan; LIU, Yi; XIE, Xiaofei; LIU, Yepang; MA, Lei; HAO, Jianye; LIU, Yang. (2021.0). *Proceedings of the 43rd International Conference on Software Engineering, Madrid, Spain, 2021 May 22-30,* (pp. 423-435) Virtual Conference: ACM. (Published)

Retrieval-augmented generation for code summarization via hybrid GNN, by LIU, Shangqing; CHEN, Yu; XIE, Xiaofei; SIOW, Jingkai; LIU, Yang. (2021.0). *Proceedings of the Ninth International Conference on Learning Representations: ICLR 2021, Vienna, Austria, May 4-8,* (pp. 1-16) Virtual Conference: (Published)

EfficientDeRain: Learning pixel-wise dilation filtering for high-efficiency single-Image deraining, by GUO, Qing; SUN, Jingyang; JUEFEI-XU, Felix; MA, Lei; XIE, Xiaofei; FENG, Wei; LIU, Yang; ZHAO, Jianjun. (2021.0). *Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI 2021), Virtual Conference, February 2-9,* (pp. 1487-1495) Washington, DC: AAAI Press. (Published)

Decision-guided weighted automata extraction from recurrent neural networks, by ZHANG, Xiyue; DU, Xiaoning; XIE, Xiaofei; MA, Lei; LIU, Yang; SUN, Meng. (2021.0). *Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI 2021), Virtual Conference, February 2-9,* (pp. 11699-11707) Virtual Conference: AAAI Press. (Published)

FakeSpotter: A simple yet robust baseline for spotting AI-synthesized fake faces, by WANG, Run; JUEFEI-XU, Felix; MA, Lei; XIE, Xiaofei; HUANG, Yihao; WANG, Jian; LIU, Yang. (2020.0). *Proceedings of the 29th International Joint Conference on Artificial Intelligence IJCAI 2020, Virtual Conference, January 7-15,* (pp. 3444-3451) Virtual Conference: ACM. (Published)

SADT: Syntax-aware differential testing of certificate validation in SSL/TLS Implementations, by QUAN, Lili; GUO, Qianyu; CHEN, Hongxu; XIE, Xiaofei; LI, Xiaohong; LIU, Yang; HU, Jing. (2020.0). *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE): Virtual, 2020 September 21-25,* (pp. 524-535) Virtual Conference: Association for Computing Machinery. (Published)

Audee: Automated testing for deep learning frameworks, by GUO, Qianyu; XIE, Xiaofei; LI, Yi; ZHANG, Xiaoyu; LIU, Yang; LI, Xiaohong; SHEN, Chao. (2020.0). *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE): Virtual, 2020 September 21-25,* (pp. 486-498) Virtual Conference: ACM. (Published)

Watch out! Motion is blurring the vision of your deep neural networks, by GUO, Qing; JUEFEI-XU, Felix; XIE, Xiaofei; MA, Lei; WANG, Jian; YU, Bing; FENG, Wei; LIU, Yang. (2020.0). *Proceedings of the 34th Conference on Neural Information Processing Systems, NeurIPS 2020, Vancouver, Canada, December 6-12,* (pp. 1-11)

Virtual Conference: NIPSF. (Published)

An empirical study on robustness of DNNs with out-of-distribution awareness, by ZHOU, Lingjun; YU, Bing; BEREND, David; XIE, Xiaofei; LI, Xiaohong; ZHAO, Jianjun; LIU, Xusheng. (2020.0). *Proceedings of the 2020 27th Asia-Pacific Software Engineering Conference (APSEC), Singapore, December 1-4,* Singapore: IEEE. (Published)

Amora: Black-box adversarial morphing attack, by WANG, Run; JUEFEI-XU, Felix; GUO, Qing; HUANG, Yihao; XIE, Xiaofei; MA, Lei; LIU, Yang. (2020.0). *Proceedings of the 28th ACM International Conference on Multimedia, MM 2020, Seattle, October 12–16,* (pp. 1376-1385) Virtual Conference: Association for Computing Machinery. (Published)

FakePolisher: Making deepfakes more detection-evasive by shallow reconstruction, by HUANG, Yihao; JUEFEI-XU, Felix; WANG, Run; GUO, Qing; MA, Lei; XIE, Xiaofei; LI, Jianwen; MIAO, Weikai; LIU, Yang; PU, Geguang. (2020.0). *Proceedings of the 28th ACM International Conference on Multimedia, MM 2020, Seattle, October 12–16,* (pp. 1217-1226) Virtual Conference: Association for Computing Machinery. (Published)

DeepRhythm: Exposing deepfakes with attentional visual heartbeat rhythms, by QI, Hua; GUO, Qing; JUEFEI-XU, Felix; XIE, Xiaofei; MA, Lei; FENG, Wei; LIU, Yang; ZHAO, Jianjun. (2020.0). *Proceedings of the 28th ACM International Conference on Multimedia, MM 2020, Seattle, October 12–16,* (pp. 4318-4327) Virtual Conference: Association for Computing Machinery. (Published)

DeepSonar: Towards effective and robust detection of AI-synthesized fake voices, by WANG, Run; JUEFEI-XU, Felix; HUANG, Yihao; GUO, Qing; XIE, Xiaofei; MA, Lei; LIU, Yang. (2020.0). *Proceedings of the 28th ACM International Conference on Multimedia, MM 2020, Seattle, October 12–16,* (pp. 1207-1216) Virtual Conference: Association for Computing Machinery. (Published)

Regression testing of massively multiplayer online role-playing games, by WU, Yuechen; CHEN, Yingfeng; XIE, Xiaofei; YU, Bing; FAN, Changjie; MA, Lei. (2020.0). *Proceedings of the 2020 IEEE International Conference on Software Maintenance and Evolution (ICSME), Adelaide, Australia, September 28 - October 2,* (pp. 692-696) Adelaide, Australia: IEEE. (Published)

Cats are not fish: Deep learning testing calls for out-of-distribution awareness, by BEREND, David; XIE, Xiaofei; MA, Lei; ZHOU, Lingjun; LIU, Yang; XU, Chi; ZHAO, Jianjun. (2020.0). *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE): Virtual, 2020 September 21-25,* (pp. 1041-1052) Virtual Conference: Association for Computing Machinery. (Published)

Marble: Model-based robustness analysis of stateful deep learning systems, by DU, Xiaoning; LI, Yi; XIE, Xiaofei; MA, Lei; LIU, Yang; ZHAO, Jianjun. (2020.0). *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering, Virtual Conference, 2020 September 21-25,* (pp. 423-435) Virtual Conference: ACM. (Published)

SPARK: Spatial-aware online incremental attack against visual tracking, by GUO, Qing; XIE, Xiaofei; JUEFEI-XU, Felix; MA, Lei; LI, Zhongguo; XUE, Wanli; FENG, Wei; LIU, Yang. (2020.0). *Proceedings of the 16th European Conference on Computer Vision, Virtual , 2020, August 23-28,* (pp. 202-219) Virtual Conference: Springer-Verlag. (Published)

How are deep learning models similar? An empirical study on clone analysis of deep learning software, by WU, Xiongfei; QIN, Liangyu; YU, Bing; XIE, Xiaofei; MA, Lei; XUE, Yinxing; LIU, Yang; ZHAO, Jianjun. (2020.0). *Proceedings of the 28th International Conference on Program Comprehension, Seoul, July 13-15,* (pp. 172-183) Seoul Republic of Korea : Association for Computing Machinery. (Published)

Towards characterizing adversarial defects of deep learning software from the lens of uncertainty, by ZHANG, Xiyue; XIE, Xiaofei; MA, Lei; DU, Xiaoning; HU, Qiang; LIU, Yang; ZHAO, Jianjun; SUN, Meng. (2020.0). *Proceedings of the 42nd International Conference on Software Engineering, Seoul, South Korea, 2020, May 23-29,* (pp. 739-751) Seoul, South Korea: Association for Computing Machinery. (Published)

Typestate-guided fuzzer for discovering use-after-free vulnerabilities, by WANG, Haijun; XIE, Xiaofei; LI, Yi; WEN, Cheng; LI, Yuekang; LIU, Yang; QIN, Shengchao; CHEN, Hongxu; SUI, Yulei. (2020.0). *Proceedings of the 42nd International Conference on Software Engineering, Seoul, South Korea, 2020, May 23-29,* (pp. 999-1010) Seoul, South Korea: Association for Computing Machinery. (Published)

MemLock: Memory usage guided fuzzing, by WEN, Cheng; WANG, Haijun; LI, Yuekang; QIN, Shengchao; LIU, Yang; XU, Zhiwu; CHEN, Hongxu; XIE, Xiaofei; PU, Geguang; LIU, Ting. (2020.0). *Proceedings of the 42nd International Conference on Software Engineering, Seoul, South Korea, 2020, May 23-29,* (pp.

765-777) Seoul, South Korea: Association for Computing Machinery. (Published)

Stealthy and efficient adversarial attacks against deep reinforcement learning, by SUN, Jianwen; ZHANG, Tianwei; XIE, Xiaofei; MA, Lei; ZHENG, Yan; CHEN, Kangjie; LIU,Yang. (2020.0). *Proceedings of 34rd AAAI Conference on Artificial Intelligence (AAAI), New York, 2020 February 7-12,* (pp. 5883-5891) New York, USA: AAAI. (Published)

DeepMutation++: A mutation testing framework for deep learning systems, by HU, Qiang; MA, Lei; XIE, Xiaofei; YU, Bing; LIU, Yang; ZHAO, Jianjun. (2019.0). *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering, San Diego, 2019 November 11-15,* (pp. 1158-1161) San Diego, California: IEEE. (Published)

Wuji: Automatic online combat game testing using evolutionary deep reinforcement learning, by ZHENG, Yan; XIE, Xiaofei; SU, Ting; MA, Lei; HAO, Jianye; MENG, Zhaopeng; LIU, Yang; SHEN, Ruimin; CHEN, Yingfeng; FAN, Changjie. (2019.0). *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering, San Diego, 2019 November 11-15,* (pp. 1-13) San Diego, California: IEEE Press. (Published)

Coverage-guided fuzzing for feedforward neural networks, by XIE, Xiaofei; CHEN, Hongxu; LI, Yi; MA, Lei; LIU, Yang; ZHAO, Jianjun. (2019.0). *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering, San Diego, 2019 November 11-15,* (pp. 1162-1165) San Diego, California: IEEE Press. (Published)

An empirical study towards characterizing deep learning development and deployment across different frameworks and platforms, by GUO, Qianyu; CHEN, Sen; XIE, Xiaofei; MA, Lei; HU, Qiang; LIU, Hongtao; LIU, Yang; ZHAO, Jianjun; LI, Xiaohong. (2019.0). *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering, San Diego, 2019 November 11-15,* (pp. 810-822) San Diego, California: IEEE Press. (Published)

A quantitative analysis framework for recurrent neural network, by DU, Xiaoning; XIE, Xiaofei; LI, Yi; MA, Lei; LIU, Yang; ZHAO, Jianjun. (2019.0). *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering, San Diego, 2019 November 11-15,* (pp. 1062-1065) San Diego, California: IEEE. (Published)

Safe inputs approximation for black-box systems, by XUE, Bai; LIU, Yang; MA, Lei; ZHANG, Xiyue; SUN, Meng; XIE, Xiaofei. (2019.0). *Proceedings of the 24th International Conference on Engineering of Complex Computer Systems, Guangzhou, China, 2019 November 10-13,* (pp. 180-189) Guangzhou, China: IEEE. (Published)

MobiDroid: A performance-sensitive malware detection system on mobile platform, by FENG, Ruitao; CHEN, Sen; XIE, Xiaofei; MA, Lei; MENG, Guozhu; LIU, Yang; LIN, Shang-Wei. (2019.0). *Proceedings of the 24th International Conference on Engineering of Complex Computer Systems, Guangzhou, China, 2019 November 10-13,* (pp. 61-70) Guangzhou, China: IEEE. (Published)

Locating vulnerabilities in binaries via memory layout recovering, by WANG, Haijun; XIE, Xiaofei; LIN, Shang-Wei; LIN, Yun; LI, Yuekang; QIN, Shengchao; LIU, Yang; LIU, Ting. (2019.0). *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Tallinn, Estonia, August 26-30,* (pp. 718-728) Tallinn, Estonia: Association for Computing Machinery. (Published)

DeepStellar: Model-based quantitative analysis of stateful deep learning systems, by DU, Xiaoning; XIE, Xiaofei; LI, Yi; MA, Lei; LIU, Yang; ZHAO, Jianjun. (2019.0). *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Tallinn, Estonia, August 26-30,* (pp. 477-487) Tallinn, Estonia: Association for Computing Machinery. (Published)

Cerebro: Context-aware adaptive fuzzing for effective vulnerability detection, by LI, Yuekang; XUE, Yinxing; CHEN, Hongxu; WU, Xiuheng; ZHANG, Cen; XIE, Xiaofei; WANG, Haijun; LIU, Yang. (2019.0). *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Tallinn, Estonia, August 26-30,* (pp. 533-544) Tallinn, Estonia: Association for Computing Machinery. (Published)

DiffChaser: Detecting disagreements for deep neural networks, by XIE, Xiaofei; MA, Lei; WANG, Haijun; LI, Yuekang; LIU, Yang; LI, Xiaohong. (2019.0). *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence, Macao, 2019 August 10-16,* (pp. 5772-5778) Macao, China: International Joint Conferences on Artificial Intelligence Organization. (Published)

DeepHunter: A coverage-guided fuzz testing framework for deep neural networks, by XIE, Xiaofei; MA, Lei; JUEFEI-XU, Felix; XUE, Minhui; CHEN, Hongxu; LIU, Yang; ZHAO, Jianjun; LI, Bo; YIN, Jianxiong; SEE, Simon;. (2019.0). *Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis, Beijing, China, 2019 July 15-19,* (pp. 146-157) Beijing, China: Association for Computing Machinery. (Published)

Cross-project defect prediction via ASTToken2Vec and BLSTM-based neural network, by LI, Hao; LI, Xiaohong; CHEN, Xiang; XIE, Xiaofei; MU, Yanzhou; FENG, Zhiyong . (2019.0). *Proceedings of the 2019 International Joint Conference on Neural Networks, Budapest, Hungary, July 14-19,* Budapest, Hungary: IEEE. (Published)

Hawkeye: Towards a desired directed grey-box fuzzer, by CHEN, Hongxu; XUE, Yinxing; LI, Yuekang; CHEN, Bihuan; XIE, Xiaofei; WU, Xiuheng; LIU, Yang. (2018.0). *CCS '18: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Toronto, October 15-19,* (pp. 2095-2108) New York: ACM. https://doi.org/10.1145/3243734.3243849 (Published)

Loopster: Static loop termination analysis, by XIE, Xiaofei; CHEN, Bihuan; ZOU, Liang; LIN, Shang-Wei; LIU, Yang; LI, Xiaohong. (2017.0). *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, Paderborn, Germany, September 4-8,* (pp. 84-94) Paderborn, Germany: Association for Computing Machinery. (Published)

Static loop analysis and Its applications, by XIE, Xiaofei. (2016.0). *Proceedings of the 24th ACM SIGSOFT Symposium on the Foundations of Software Engineering, Seattle, November 13-18, 2016,* (pp. 1130-1132) Seattle, WA, USA: Association for Computing Machinery. (Published)

Proteus: Computing disjunctive loop summary via path dependency analysis, by XIE, Xiaofei; CHEN, Bihuan; LIU, Yang; LE, Wei; LI, Xiaohong. (2016.0). *Proceedings of the 24th ACM SIGSOFT Symposium on the Foundations of Software Engineering, Seattle, November 13-18, 2016,* (pp. 61-72) Seattle, WA, USA: Association for Computing Machinery. (Published)

S-Looper: Automatic summarization for multipath string loops, by XIE, Xiaofei; LIU, Yang; LE, Wei; LI, Xiaohong; CHEN, Hongxu. (2015.0). *Proceedings of the 2015 International Symposium on Software Testing and Analysis, Baltimore, July 13-17,* (pp. 188-198) Baltimore, MD, USA: Association for Computing Machinery. (Published)

Research Grants

Singapore Management University

Evaluating the Perception Module in Autonomous Driving Systems: Impact on Vehicle Motion, Academic Research Fund (AcRF) Tier 2, Ministry of Education (MOE) , PI (Project Level): XIE Xiaofei, 2024, S$723,333

Towards Building Unified Autonomous Vehicle Scene Representation for Physical AV Adversarial Attacks and Visual Robustness Enhancement (Stage 1a), AI Singapore Robust AI Grand Challenge, AI Singapore , Co-PI (Project Level): XIE Xiaofei, 2023, S$2,995,800

Trustworthy AI Centre NTU (TAICeN), Cyber Security Agency of Singapore (CSA) , Co-PI (Project Level): XIE Xiaofei, SUN Jun, 2023

Automatic non-linear loop summarization and its applications, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): XIE Xiaofei, 2021, S$100,000

Other Institutions

From Risk Identification to Risk Management: A Systematic Approach to Mitigating LLM Supply Chain Risks, CRPO Grant Call - Translation and Innovation Grants, CRPO PI (Project Level): XIE Xiaofei, 2025, SGD1,499,940

Towards Building Unified Autonomous Vehicle Scene Representation for Physical AV Adversarial Attacks and Visual Robustness Enhancement, AISG, AI Singapore - Robust AI Grand Challenge Co-PI (Project Level): XIE Xiaofei, 2023, SGD2,995,800

TRUSTWORTHY AI CENTRE NTU (TAICeN), NCRP, Cyber Security Agency of Singapore Co-PI (Project Level): XIE Xiaofei, 2022, SGD12,364,100

TEACHING

Courses Taught

Singapore Management University

Undergraduate Programmes :

Enterprise Solution Development

Foundations of Cybersecurity

Postgraduate Professional Programmes :

Capstone Project - Software and Cyber-Physical Systems

Postgraduate Research Programmes :

Empirical Research Project 1

Empirical Research Project 2

Empirical Research Project 3

Empirical Research Project 4

OTHER ACADEMIC AND PROFESSIONAL ACTIVITIES

Consultancy

MetaTrust Labs Pte. Ltd, Nov 2023 - Oct 2025

Media Contributions and Citations

TikTok, A New Political Weapon: Can It Be Moderated?, Channel News Asia, 25 May 2023
https://youtu.be/U6FvLqVtUnE

UNIVERSITY SERVICE

Singapore Management University

Organize a hacking workshop for VJC students, Hacking Workshop for VJC Students, Dec 2022

Organized a professor team and competed against the student teams on hard coding problems. , SCIS DAY and Tic Tac Code, Oct 2022

EXTERNAL SERVICE – PROFESSIONAL

Committee Chair, Program Committee, ICECCS25 ISACE 25, 2025

Committee Member, Program Committee, ISSTA 25, ASE 25, ICSE 25, WWW 25, ICSE-NIER 25, ICLR 25, ICML 25, AAAI 25, 2025 - 2026

Workshop Organizer, the 3rd Workshop on AI and Software Testing/Analysis , 2024

Editor Associate Editor, Journal of Evolution and Process, 2024 - Present

Committee Member, Program Committee, ISSTA, 2024, NeurIPS 2024, ISSRE 2024, AISec 2024, ICML 2024, FSE Student Research Competition 2024, 2024 - Present

Conference Local Chair, Local Chair, ATVA and PRDC, 2023 - Present

Committee Member, ESEC/FSE SRC & Artifacts 2023, ISSRE 2023, MSR 2023, ASE 2023, ICSE Posters Track 2023 ICCV 2023, ICLR 2023, PRDC 2023, 2023

Guest Editor, IEEE TDSC Special Issue “SI-Reliability and Robustness in AI-Based Cybersecurity Solutions” , 2022 - Present

Workshop Organizer, Machine Learning Techniques for Software Quality Evaluation (MaLTeSQuE) , 2022

Editor Associate Editor, Frontiers in Computer Science, 2022 - Present

Workshop Organizer, AI and Software Testing/Analysis (AISTA) , 2022

Reviewer Conference Paper, International Symposium on Software Reliability Engineering (ISSRE) , 2022

Project sponsor, ICSE SCORE 2023, 2022 - Present

Presenter Keynote Address, SEAIS, 2022

Reviewer Conference Paper, ASE ACM Student Research Competition, ESEC/FSE Artifacts, ICCV, AAAI, ICLR, SETTA, 2022 - Present

Reviewer Journal Article, TDSC, TSE, TOSEM, JSS, ACM Computing Surveys, 2022 - Present

Editor Associate Editor, Frontiers in Big Data, 2021 - 2022

EXTERNAL SERVICE – PUBLIC SECTOR AND COMMUNITY SERVICE

Committee Member, Artificial Intelligence Technical Committee, Artificial Intelligence Technical Committee, 2023 - Present

Discussant, AISG Grant Call Workshop on Misinformation Discrimination, AISG , 2022