Simin Chen

+1 214-3569-114
https://www.siminchen.site
https://github.com/SeekingDream
sxc180080@utdallas.edu

Research Interests

My research focuses on **Software Engineering**, and **Machine Learning**, with the goal of designing foundational infrastructure tools to make ML-based systems more reliable, interpretable, and efficient. To achieve such a goal, I developed techniques to improve the quality of ML systems at three stages. (1) At the ML model development stage, I design tools to explain the decision-making of ML models and apply the explanation results to locate/debug the bugs in the models; (2) at the ML model deployment stage, I develop tools to quantify the privacy leakage risk of ML models and optimize the ML model performance; (3) at the ML model runtime stage, I develop tools for validating the inputs of ML models to improve the model efficiency.

Education

Postdoc Researcher — Sep. 2024 –
Columbia University (Advisor: **Dr. Baishakhi Ray**) — New York, The United States

Ph.D. Candidate | ***(GPA 3.82/4.0)*** — Jan. 2019 – Aug. 2024
University of Texas at Dallas (Advisor: **Dr. Wei Yang**, and **Dr. Cong Liu**) — Dallas, The United States

Master of Science | ***(GPA 84.7/100)*** — Sep. 2015 – Jun. 2018
Tongji University — ShangHai, China

Bachelor of Science | ***(GPA 4.48/5.0)*** — Sep. 2011 – Jun. 2015
Tongji University — ShangHai, China

Publication

I have authored and published twelve technical track papers, one journal paper, and one poster paper. Notably, I served as the lead author for **ten** of the technical track papers, with six of them being featured in prestigious software engineering conferences, including ESEC/FSE (four times), ISSTA, and ASE. Additionally, four of my first authored papers were accepted in high-impact artificial intelligence conferences, namely ICML, CVPR (twice) and IJCAI. Moreover, I am the corresponding author of one journal paper (TOSEM 2024) and one conference paper (ACL 2023).

(C16) **Simin Chen**, Pranav Pusarla, Baishakhi Ray. DyCodeEval: Dynamic Benchmarking of Reasoning Capabilities in Code Large Language Models Under Data Contamination. In Proceedings of the 42nd International Conference on Machine Learning (ICML 2025)

(C15) Ravishka Rathnasuriya, Tingxi Li, Zexin Xu, Zihe Song, Mirazul Haque, **Simin Chen**, Wei Yang (2025). SOK: Efficiency Robustness of Dynamic Deep Learning Systems. In Proceedings of the 34th USENIX Security Symposium (Usenix Security 2025)

(C14) Dezhi Ran, Yuan Cao, Yuzhe Guo, Yuetong Li, Mengzhou Wu, **Simin Chen**, Wei Yang, Tao Xie. Medusa: A Framework for Collaborative Development of Foundation Models with Automated Parameter Ownership Assignment. In Proceedings of the 33th ACM International Conference on the Foundations of Software Engineering (FSE 2025)

(J3) Haibo Yu, Xiaohong Han, **Simin Chen**, Xiaoning Feng, Guangzhao Sun and Wei Yang. DPEfficR: a data and parameter efficient approach for training neural API recommendation model. Automated Software Engineering Journal (ASE-J 2025)

(C13) Jiaqi Wu, Simin Chen, Jing Tang, Yuzhe Yang, Yiming Chen, Lixu Wang, Song Lin, Zehua Wang, Wei Chen, Zijian Tian. FDPT: Federated Discrete Prompt Tuning for Black-Box Visual-Language Models. In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV 2025).

(C12) **Simin Chen**, XiaoNing Feng, Xiaohong Han, Cong Liu, and Wei Yang. PPM: Automated Generation of Diverse Programming Problems for Benchmarking Code Generation Models. In Proceedings of the 32nd ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2024).

(C11) **Simin Chen**, Zexin Li, Wei Yang, and Cong Liu. Decix: Explain Deep Learning-Based Code Generation Applications. In Proceedings of the 32nd ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2024).

(J2) XiaoNing Feng, Xiaohong Han, **Simin Chen**, Cong Liu, and Wei Yang. LLMEffiChecker: Understanding and Testing Efficiency Degradation of Large Language Models. ACM Transactions on Software Engineering and Methodology (TOSEM 2024).

(J1) Jaeseong Lee, Simin Chen, Austin Mordahl, Cong Liu, Wei Yang, and Shiyi Wei. Automated Testing Linguistic Capabilities of NLP Models. ACM Transactions on Software Engineering and Methodology (TOSEM 2024).

(C10) **Simin Chen**, Hanlin Chen, Mirazul Haque, Cong Liu, Wei Yang. The Dark Side of Dynamic Routing Neural Networks: Towards Efficiency Backdoor Injection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2023).

(C9) Zexin Li, Bangjie Yin, Taiping Yao, Junfeng Guo, Shouhong Ding, **Simin Chen**, Cong Liu. Sibling-Attack: Rethinking Transferable Adversarial Attacks against Face Recognition In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2023).

(C8) **Simin Chen**, Shiyi Wei, Cong Liu, Wei Yang. DyCL: Dynamic Neural Network Compilation Via Program Rewriting and Graph Optimization. In Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2023).

(C7) **Simin Chen**, Cong Liu, Mirazul Haque, Zihe Song, and Wei Yang. NMTSloth: understanding and testing efficiency degradation of neural machine translation systems. In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2022).

(C6) Yiming Chen, **Simin Chen**, Zexin Li, Wei Yang, Cong Liu, Robby T. Tan, Haizhou Li. Dynamic Transformers Provide a False Sense of Efficiency. In Proceedings of the 61st Association for Computational Linguistics (ACL 2023)

(C5) Mirazul Haque, Rutvij Shah, **Simin Chen**, Berrak Sisman, Cong Liu, Wei Yang. SlothSpeech: Denial-of-service Attack Against Speech Recognition Models. In Proceedings of the 24th INTERSPEECH Conference (INTERSPEECH 2023).

(C4) **Simin Chen**, Mirazul Haque, Cong Liu, and Wei Yang. 2022a. DeepPerform: An Efficient Approach for Performance Testing of Resource-Constrained Neural Networks. In Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering (ASE 2022).

(C3) **Simin Chen**, Hamed Khanpour, Cong Liu, and Wei Yang. 2022b. Learning to Reverse DNNs from AI Programs Automatically. In Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence (IJCAI 2022).

(C2) **Simin Chen**, Zihe Song, Mirazul Haque, Cong Liu, and Wei Yang. NICGSlowDown: Evaluating the Efficiency Robustness of Neural Image Caption Generation Models. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2022).

(C1) **Simin Chen**, Soroush Bateni, Sampath Grandhi, Xiaodi Li, Cong Liu, and Wei Yang. DENAS: Automated Rule Generation by Knowledge Extraction from Neural Networks. In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2022).

(P1) Hanlin Chen, **Simin Chen**, Wenyu Li, Wei Yang, Yiheng Feng. Impact Analysis of Inference Time Attack of Perception Sensors on Autonomous Vehicles. In Proceedings of the Transportation Research Board Annual Meeting (TRB 2023)

Scholarships and Awards

- David Daniel Thesis Award 2025 (awarded to only two recipients university-wide each year)
- Second prize in THUBA DAO Global Hackson for Blockchain Competition (2000 USD).
- Travel grant award from CVPR 2022.
- Travel grant award from SIGSoft ISSTA 2023.

Industry Experience

NEC Laboratories America

Member of System Security and Reliability Team — January 2020 – May 2020

- Participate in the Graph-based Source Code Vulnerability Detection

Microsoft Research

Member of System Security and Reliability Team — May 2021 – July 2021

- Participate in the project of reverse engineering on on-device DNNs

Amazon Web Services

Member of Automated Reasoning Group — May 2023 – August 2023

- Participate in the project of leveraging large language model for *Cedar* language verification

Teaching Experience

University of Texas at Dallas

CS 4393 – Computer and Network Security

CS 4347 – Computer Engineering

SE 4367 - Software Testing Verification Validation and Quality Assurance

SE 6387 - Advanced Software Engineering Project (Graduate Course)

CS 6301 – Special Topics in Computer Science (Graduate Course)

MENTORING

I have had the fortunate opportunity to mentor and collaborate with the following students.

- Haibo Yu (B.S., Taiyuan University of Technology; Co-authored [paper under submission])
- Xiaoning Feng (B.S., Taiyuan University of Technology; Co-authored [paper under submission])
- Yixin He (B.S., University of Southern California; Co-authored [paper under submission])
- Wenyu Li (MS, University of Electronic Science and Technology of China; Co-authored)
- Sampath Grandhi (MS, UTD; Co-authored)
- Zihe Song (Ph.D., UTD; Co-authored)
- Miao Miao (Ph.D., UTD)
- Hashmi Junaid (MS, UTD)
- Seo Jeongwon (MS, UTD)
- Zexin Li (Ph.D., University of California at Riverside; Co-authored)
- Yufei Li (Ph.D., University of California at Riverside; Co-authored [paper under submission])
- Yiming Chen (Ph.D., Nanyang Technological University; Co-authored)

SERVICE

Software Engineering Community

- **Program Committee**, International Conference on Automated Software Engineering (ASE 2024, 2025).
- **Junior Program Committee**, Conference on Mining Software Repositories (MSR 2023).
- **Reviewer**, International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2023, 2024).
- **Sub-Reviewer**, International Conference on Software Engineering (ICSE 2021, 2023).
- **Sub-Reviewer**, Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2022, 2024)
- **Sub-Reviewer**, International Conference on Automated Software Engineering (ASE 2022, 2023)
- **Sub-Reviewer**, The International Symposium on Software Reliability Engineering (ISSRE 2022, 2023)
- **Sub-Reviewer**, International Conference on Software Testing, Verification and Validation (ICST 2022, 2023, 2024).

Artificial intelligence and Machine Learning Community

- **Program Committee**, Neural Information Processing Systems (NeurIPS 2025).
- **Program Committee**, International Conference on Machine Learning (ICML 2025).
- **Program Committee**, International Conference on Learning Representations (ICLR 2025).
- **Program Committee**, Annual Meeting of the Association for Computational Linguistics (ACL 2025).
- **Program Committee**, Conference on Empirical Methods in Natural Language Processing (EMNLP 2025).
- **Program Committee**, Computer Vision and Pattern Recognition Conference (CVPR 2023, 2024, 2025).
- **Program Committee**, Association for the Advancement of Artificial Intelligence (AAAI 2023, 2024, 2025).
- **Program Committee**, Winter Conference on Applications of Computer Vision (WACV 2022).
- **Program Committee**, International Conference on Computer Vision (ICCV 2023, 2025).
- **Program Committee**, European Conference on Computer Vision (ECCV 2022).
- **Program Committee**, International Association for Pattern Recognition (ICPR 2024).

TALKS

Conference Talks and Posters

- The Dark Side of Dynamic Routing Neural Networks: Towards Efficiency Backdoor Injection at **CVPR 2023** (Virtual)
- DyCL: Dynamic Neural Network Compilation Via Program Rewriting and Graph Optimization at **ISSTA 2023** (Seattle, Washington, USA).
- NMTSloth: Understanding and Testing Efficiency Degradation of Neural Machine Translation Systems at **ESEC/FSE 2022** (Virtual)
- DeepPerform: An Efficient Approach for Performance Testing of Resource-Constrained Neural Networks at **ASE 2022** (Oakland Center, Michigan, USA)
- Learning to Reverse DNNs from AI Programs Automatically at **IJCAI 2022** (Virtual)
- NICGSlowDown: Evaluating the Efficiency Robustness of Neural Image Caption Generation Models at **CVPR 2022** (New Orleans, Louisiana, USA)
- DENAS: Automated Rule Generation by Knowledge Extraction from Neural Networks at **ESEC/FSE 2020** (Virtual)

OPEN-SOURCE CONTRIBUTIONS

I led the development of six tools/datasets for improving the efficiency and security of Machine Learning Systems.

- **DyCL:** DyCL is a tool for compiling dynamic neural networks. It could help to deploy dynamic neural networks efficiently on different hardware platforms. It is available at https://github.com/SeekingDream/ISSTA23_DyCL
- **DENAS:** DENAS is an automatic tool that can extract knowledge from neural networks and represent the knowledge as explainable rules. DENAS can help model developers locate and debug the errors in the ML models. It is available at https://github.com/SeekingDream/FSE20_DENAS.
- **NICGSlowDown:** NICGSlowDown is a tool that generates test inputs to test neural image caption systems. It is available at https://github.com/SeekingDream/CVPR22_NICGSlowDown
- **NMTSloth:** NMTSloth is a tool that generates test inputs to test neural machine translation systems. It is available at https://github.com/SeekingDream/FSE22_NMTSloth
- **NNReverse:** NNReverse is a large scale binary code dataset, which is compiled from different neural network architectures using different compiler settings. It is available at Google Drive Link
- **DeepPerform:** DeepPerform is a learning-based testing tool to test dynamic neural networks. It automatically learns the buggy inputs' distribution and generates test generation with only 6-10 milliseconds. It is available at https://github.com/SeekingDream/DeepPerform

SKILLS

Programming: Python (Pytorch, Tensorflow), MATLAB, C/C++ , Java
Program Analysis Tool: Angr, Joern
DL Techniques: NLP, Uncertainty Analysis, Explainable ML, Energy-efficient DNN