Taoran Li

College Station, TX, US| PETR 359
Tel: +1-2178199251 | Email: taoranl2@illinois.edu | Web: taoranl2.github.io

EDUCATION

Texas A&M University **College Station, TX, US**
Doctor of Philosophy in Computer Science *Jan. 2026-present*
Advisor: Prof. Zhiyuan Yu

University of Illinois at Urbana-Champaign **Urbana, IL, US**
Master of Engineering in Computer Engineering *Aug. 2023-Dec. 2024*
Advisor: Prof. Varun Chandrasekaran
Bachelor of Science in Computer Engineering *Aug. 2018-Jun. 2023*

Zhejiang University **Hangzhou, Zhejiang, China**
Bachelor of Engineering in Computer Engineering *Aug. 2018-Jun. 2023*

Research Interests:
Computer Security & Privacy, Trustworthy Machine Learning, AI Safety, Applied Cryptography

APPOINTMENTS

University of Illinois at Urbana-Champaign, US *Feb. 2025-Dec. 2025*
Academic Hourly Employee
Advisor: Prof. Varun Chandrasekaran

PUBLICATIONS

- Xiaomin Li*, Mingye Gao*, Yuexing Hao, **Taoran Li**, Guangya Wan, Zihan Wang, Yijun Wang. MedGUIDE: Benchmarking Clinical Decision-Making in Large Language Models. arXiv https://arxiv.org/abs/2505.11613. Under review at NeurIPS 2025.
- Qilong Wu*, **Taoran Li***, Tianyang Zhou*, Varun Chandrasekaran. SoK: Understanding (New) Security Issues Across AI4Code Use Cases. Under review at USENIX Security Symposium 2026. arXiv available soon.
- Hengrui Jia, **Taoran Li**, Jonas Guan, Varun Chandrasekaran. The Metric Mirage: A False Sense of Unlearning. Under review at USENIX Security Symposium 2026. arXiv available soon.

RESEARCH

Concept Unlearning in Large Language Model *Jun. 2024-Aug.2025*
- Collaborating with Prof. Varun Chandrasekaran and Hengrui Jia to develop a framework for removing user-specified information from large language models (LLMs) while preserving model utility.
- Identified unique concepts within sensitive datasets using semi-supervised clustering, focusing on data unique to specific documents while ensuring minimal overlap with other training data.
- Designed and applied targeted unlearning algorithms to eliminate sensitive conceptual information rather than entire documents, significantly reducing utility degradation.
- Conducted evaluations on datasets, including positive, negative, and fan fiction data, to validate the effectiveness of the framework and minimize residual knowledge.

SoK: AI for Code *Mar. 2025- Aug. 2025*
- Collaborating with Tianyang Zhou, Qilong Wu and Prof. Varun Chandrasekaran
- Investigating and summarizing techniques and security & privacy issues for leveraging AI in code generation, vulnerability detection and code translation
- Giving insights for future study on security & privacy of AI4Code
- To be submitted to USENIX Security Symposium 2026

Zk-SNARK (Gnark) for Secure String Matching *Aug. 2024-Dec. 2024*
- Directed by Prof. Yupeng Zhang to develop a platform for secure string matching using zk-SNARKs (Zero-

Knowledge Succinct Non-Interactive Arguments of Knowledge) to monitor and prevent sensitive information leaks.

- Leveraged the gnark library to generate efficient verifiable proofs for private data verification without exposing sensitive details.
- Optimized performance using a sliding window technique and the Rabin–Karp algorithm to efficiently detect string matches, reducing time complexity.
- arXiv https://arxiv.org/abs/2505.13964

PROJECTS

Checking Consistency Is Not Good Enough *Jan. 2024-May. 2024*

- This project focuses on addressing the vulnerabilities of the existing MPC frameworks, particularly in detecting and mitigating data poisoning attacks that can compromise the outcomes of collaborative machine learning efforts. Platforms like Cerebro fall short in identifying malicious datasets introduced prior to computation.
- Presented four potential solutions: 1) Auditor, introducing an auditor which performs as a trusted third party to evaluate the data based on; 2) Anomaly Detection and Outlier Analysis, using Normalizing Flows to detect outlier poisoned data; 3) SISA training, introducing the definition of shard, presenting shards incrementally and evaluating loss. Experiments showed that normalization flow could distinguish the poisoned dataset from benign ones.
- Made presentation about this project in the class directed by Prof. Varun Chandrasekaran

A Comprehensive Survey on Secure Machine Learning *Jan. 2024-May. 2024*

- Make a comprehensive survey on the interaction between secure multi-party computation and the area of machine learning. This review explores key contributions that leverage MPC to enable multiple parties to engage in ML tasks without compromising the privacy of their data. The study also explores an innovative application domain for SecureML techniques: the integration of these methodologies in gaming environments utilizing ML.
- Made a presentation about this topic in the class directed by Prof. David Heath
- arXiv https://arxiv.org/abs/2505.15124

A Comprehensive Survey on Trustworthy Machine Learning with Privacy and Security *Sep. 2023-Dec. 2023*

- Make a comprehensive survey on the topic of trustworthy machine learning with privacy and security, including topic in data privacy, membership inference attack, privacy risks of ML, model explanation and machine unlearning
- Made presentation about this topic in the class directed by Prof. Han Zhao

A Desktop-Size Environment-Controlled Greenhouse for Multi-Variable Optimization of Crop Growth
Feb. 2023-Jun. 2023

- Design a desktop-size environment-controlled greenhouse with reduced size and energy consumption that can be used for ordinary customers as a senior design project directed by Prof. Wee-Liat Ong
- The light, air circulation, temperature and humidity could be shown and controlled through mobile app

TEACHING ASSISTANT EXPERIENCE

- Math 241 (Calculus III) With Prof. Thomas Honold *Fall 2022*
- Math 285 (Differential Equations) With Prof. Thomas Honold *Spring 2023*

Be responsible for leading discussion section, holding office hours, grading homework & exam papers

SERVICES

Reviewer: NeurIPS 2025, ACL 2026

ADDITIONAL INFORMATION

Activities: Member, Student Union, ZJU *Oct. 2018-Oct. 2019*
Volunteer Teaching in Guilin, Guangxi Province, China *Summer, 2019*
Class President in Computer Engineering
Presented with Student Leadership Award in 2018-2019

Language: Python, C, C++, System Verilog, HTML, CSS, JavaScript, LC-3, x86 Assemble, MATLAB, SQL

Tools: PyTorch, Latex, Git, CUDA