Taoran Li

Urbana, IL, US| Tel: +1-2178199251 | Email: taoranl2@illinois.edu

Looking for a PhD position in Computer Security &Privacy

EDUCATION

University of Illinois at Urbana-Champaign (UIUC), US *Expected Dec.2024*

Master of Engineering in Computer Engineering

University of Illinois at Urbana-Champaign (UIUC), US *Sept.2018-Jun. 2023*

Bachelor of Science in Computer Engineering

Zhejiang University (ZJU), China *Sept.2018-Jun. 2023*

Bachelor of Engineering in Computer Engineering

Related Coursework:

Computer Security, Cryptography, Machine Learning with Privacy, Secure Multi-party Computation

RESEARCH

Concept Unlearning in Large Language Model *Jun.2024-Present*

- Developed a comprehensive framework for concept unlearning to remove sensitive information from large language models (LLMs).
- Identify unique concepts within sensitive datasets, followed by targeted unlearning to eliminate specific data points while preserving model utility.
- Leveraging positive, negative, and fan fiction datasets, I conducted detailed evaluations to validate unlearning effectiveness and minimize residual knowledge.
- Work with Nick (Hengrui) Jia and Prof. Varun Chandrasekaran, to be submitted to IEEE Symposium on Security and Privacy 2025.

Zk-SNARK (Gnark) for String Match *Aug.2024-Present*

- Working on developing a platform using Gnark for string matching to monitor and prevent sensitive information leaks for companies.
- Directed by Prof. Yupeng Zhang

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

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

Shooting Game Development on Unreal Engine 4 *Feb.2022-May. 2022*

- Developed a shooting game with random enemies and occupation target. Players need to stay in an assigned place for a certain period to get enough points to win the game and cannot be killed by enemies during this time. The game's enemies get more and more powerful as you move up the levels.
- Be responsible for the enemy's movement, attack and sound.

Unix-Like Computer System Development *Feb.2022-May. 2022*

- Developed the core of a Unix-like operating system using C, C++ and x86 Assemble
- Developed the software used to interface between devices and applications, i.e., operating systems
- Be responsible for the part of Interrupt Description Table and system call between the kernel and user
- Designed a mouse cursor and left/right click for terminal change

Applied Parallel Programming and GPU Optimizations *Aug.2021-Dec.2021*

- Implemented and optimizing the forward-pass of a convolutional layer using CUDA
- Made GPU optimizations of the kernel in the following aspects: Tiled shared memory convolution; Shared memory matrix multiplication and input matrix unrolling; Kernel fusion for unrolling and matrix-multiplication; Weight matrix (kernel values) in constant memory; Sweeping various parameters to find best values (block sizes, thread coarsening); Multiple kernel implementations for different layer sizes

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

ADDITIONAL INFORMATION

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

Language: Chinese (native), English (Fluent)

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

Tools: PyTorch, Latex, Git, CUDA