

EDUCATION

-
- University of Michigan, Ann Arbor**

 - *Ph.D. in Computer Science and Engineering*
 - Courses: Advanced Operating Systems, Advanced Compiler*

Ann Arbor, USA

Sep 2024 - Present
 - Carnegie Mellon University**

 - *M.Sc. in Artificial Intelligence Engineering – Information Security*
 - Courses: Trustworthy AI Autonomy, Internet Services, Telecommunication Networks, Advanced Natural Language Processing*
 - Thesis: Cybersecurity Challenges in the Age of AI: New Attack and Defense Opportunities*

Pittsburgh, USA

Sep 2022 - May 2024
 - The Chinese University of Hong Kong, Shenzhen**

 - *B.Eng. in Computer Science and Engineering*
 - Courses: Distributed and Parallel Computing, Cloud Computing, Database System, Data Structures and Algorithms*

Shenzhen, China

Sep 2018 - Jun 2022

RESEARCH INTERESTS

Robust and trustworthy AI. Secure machine learning system.

PUBLICATIONS

-
- **J. Li**, J. Brewington, Q. Zhang, Z.M. Mao. WIP: Hijacking Attacks on UAV Follow-Me Systems in Realistic Scenarios. *The 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec'25)*, 2025.
 - **J. Li**, Y. Yuan, Z. Zhang. Enhancing LLM Factual Accuracy with RAG to Counter Hallucinations: A Case Study on Domain-Specific Queries in Private Knowledge-Bases. *arXiv*, 2024.
 - P. Sharma, **J. Li**, and G. Joshi. On Improved Distributed Random Reshuffling Over Networks. *In Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2023.
 - T. Kim, **J. Li**, N. Madaan, S. Singh, and C. Joe-Wong. Adversarial Robustness Unhardening via Backdoor Attacks in Federated Learning. *In NeurIPS 2023 Workshop on Backdoors in Deep Learning*, 2023.

RESEARCH EXPERIENCES

-
- Robust AI-Driven UAV system**

 - *Advisor: Prof. Morley Mao, Robustnet, UMich*
 - Developed UAV target following systems driven by modern deep learning object tracking algorithms (motion-based, appearance-based, and hybrid), which is deployed on a DJI Matrice drone and custom NUC computing unit
 - Demonstrated system robustness in following a target under diverse benign scenarios (windy, textured environment, random target motion) and system vulnerability in adversarial contexts with flight control stack and physical simulator
 - Discovered that a sophisticated attacker can cause the following target to switch to a selected object with over 80% attack success rate and proposed using camera motion compensation algorithm to improve robustness under attack.

Ann Arbor, USA

Sep 2024 - Present
 - Retrieval-Augmented Generation LLM**

 - *Advisor: Prof. Graham Neubig, CMU*
 - Designed a RAG LLM system (online dataset generator, embedding, vector database, and LLM serving) to reduce LLM hallucinations when performing question-answer on private dataset
 - Discovered RAG LLM achieves the best factual accuracy with finetuned embedding (0.437 Recall, 0.304 F1 Score) and the limitation of finetuning core LLM on small scale dataset [code]

Pittsburgh, USA

Sep 2023 - Feb 2024
 - Secure Federated Learning System**

 - *Advisor: Prof. Carlee Joe-Wong, LIONS Group, CMU*
 - Improved the security of federated (distributed) learning system under the scenario of adversarial participating clients through central server aggregation algorithms.
 - Designed and implemented a novel attack, reducing model robustness against evasion attacks by 89.73%
 - Developed a modularized attack pipeline, which reduced the code complexity by 57.47% [code]

Pittsburgh, USA

Sep 2022 - May 2024
 - Distributed Optimization over Networks**

 - *Advisor: Prof. Gauri Joshi, OPAL Lab, CMU*
 - Designed experiments to show that non-convex convergence exposes a gap in theory
 - Implemented network graphs, optimizers, and gradient tracking while recovering literature results from scratch [code]
 - Improved the theoretical convergence results of the decentralized random reshuffling algorithm under convex and non-convex cases

Pittsburgh, USA

Jan 2023 - Aug 2023

WORK EXPERIENCES

- **Multilingual Natural Language Processing** Shenzhen, China
Software Engineer Aug 2021 - Aug 2022
 - Preprocessed and augmented large-scale (10 million) African language corpus through tokenization and back-translation
 - Upgraded THUMT NLP toolkit, by adding multilingual NN, denoising auto-encoder functionalities while keeping monolingual setting performance BLEU 26.85
 - Won 1st place in the WMT22 competition by achieving the best BLEU 14.09 and ChrF++ 37.42 [code]
- **Agriculture IoT System** Shenzhen, China
Programming Lead Nov 2019 - Aug 2021
 - Designed a farm data collection system using Arduino chips, sensors, a base station, and a Raspberry Pi server
 - Built a manager website, with Go backend, Vue.js frontend, and AWS QLDB database
 - Deployed the system to a Shenzhen farm and won the Bronze Medal in entrepreneurship competition [link]

SELECTED PROJECTS

- **Chain-of-Thought Program Analysis** Feb 2023
 - Evaluated GPT-3.5 and GPT-4's zero shot performance on predicting, (1) the output (2) special character vulnerability, of synthetic python program using chain-of-thought reasoning
 - Discovered that the prediction accuracy drops below 50% when the program gets longer (>10 lines) and chain-of-thought improve the accuracy on medium programs (10-15 lines) by 10% while failing on longer programs
- **Performance Evaluation on Log-Structured Key-Value Store** Feb 2023
 - Implemented log-structured memory management, failure recovery, testing workload, and a baseline naive-KV-store [code]
 - Concluded that log-KV-store outperforms by 48.28% in recovery throughput and 77.48% in recovery error [paper]
- **System Memory Management for Malloc and Free** Feb 2023
 - Improved throughput by 66.17% by selecting policies, including first-two-fit and LIFO, for block searching and insertion
 - Optimized memory utilization by 24.11% at the bit level, by reducing external and internal fragmentation
- **University Sports Association App** Feb 2021
 - Led the five-developer team to build an administration mini-program using Vue and NoSQL database
 - Designed the cloud API location check-in functionality to reduce the client computational burden and speedup the program
 - Achieved simultaneous mobile phone access, data transmission, and GPS locating of over 100 users in activities

TEACHING EXPERIENCES

- **Introduction to Computer System, CMU** Pittsburgh, USA
Teaching Assistant Aug 2023 - May 2024
 - Covered topics including, assembly, c programming, and computer architecture
- **Mathematical Foundations for AI, CMU** Pittsburgh, USA
Teaching Assistant June 2023 - Aug 2023
 - Covered linear algebra topics including matrix, linear transformation, vector spaces, and eigenvalues
- **Adversarial Machine Learning, CMU** Pittsburgh, USA
Teaching Assistant Jan 2023 - May 2023
 - Covered topics including supervised spam filtering, unsupervised network anomaly detection, and adversarial deep learning

SKILLS

Python, C/C++, SQL, Pytorch, Git, Docker, Linux, Arduino, CUDA, Verilog

HONORS AND AWARDS

- WMT22 Large-Scale Machine Translation for African Languages - Constrained Track, 1st Place Sep 2022
- China International "Internet +" Entrepreneurship Competition, Bronze Medal (1%) Aug 2021
- Diligentia College Scholarship of CUHK Shenzhen (5% of a thousand students) Sep 2020