Jiarui Li Website, Linkedin Email: jiaruili@umich.edu Mobile:+1-412-915-6531

Education

- **University of Michigan, Ann Arbor** Ann Arbor, USA
  Ph.D. in Computer Science and Engineering *Sep 2024 - Present*
  Courses: *Advanced Computer Network, Advanced Operating Systems*
- **Carnegie Mellon University** Pittsburgh, USA
  M.Sc. in Artificial Intelligence Engineering – Information Security *Sep 2022 - May 2024*
  Courses: *Trustworthy AI Autonomy, AI in Info Security, Internet Services, Telecommunication Networks, Machine Learning*
  Thesis: *Cybersecurity Challenges in the Age of AI: New Attack and Defense Opportunities*
- **The Chinese University of Hong Kong, Shenzhen** Shenzhen, China
  B.Eng. in Computer Science and Engineering *Sep 2018 - Jun 2022*
  Courses: *Distributed and Parallel Computing, Cloud Computing, Database System, Operating System, Data Structures and Algorithms*

Publications

- 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. [paper]
- 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. [paper]
- W. Jiao, Z. Tu, **J. Li**, W. Wang, J. tse Huang, and S. Shi. Tencent's multilingual machine translation system for wmt22 large-scale African languages. *In Proceedings of the Seventh Conference on Machine Translation*, 2022. [paper]

Research Experiences

- **Secure Autonomous Systems (WIP)** Ann Arbor, USA
  Advisor: Prof. Morley Mao, Robustnet, UMich *Sep 2024 - Present*
  ○ Studying vulnerabilities of SLAM algorithms against attacks, emphasizing localization errors caused by map inconsistencies
  ○ Analyzing acoustic laser-based attacks targeting camera perception in UAVs against downstream computer vision algorithms
- **Secure Federated Learning** Pittsburgh, USA
  Advisor: Prof. Carlee Joe-Wong, LIONS Group, CMU *Sep 2022 - May 2024*
  ○ Designed and implemented a novel attack, reducing model robustness against evasion attacks by 89.73%
  ○ Proposed the selective model extraction strategy, a practical attack initialization, which achieves 36.4% acceleration
  ○ Independently developed an attack pipeline with devised modularity, which reduced the code complexity by 57.47% [code]
- **Distributed Optimization over Networks** Pittsburgh, USA
  Advisor: Prof. Gauri Joshi, OPAL Lab, CMU *Jan 2023 - Aug 2023*
  ○ Designed experiments to show that non-convex convergence exposes a gap in theory
  ○ Analyzed and concluded that the averaged gradient norm will be dominant by the decentralized network consensus error
- **Multilingual Natural Language Processing** Shenzhen, China
  Mentor: Dr. Wenxiang Jiao, AI Lab, Tencent Co. *Aug 2021 - Aug 2022*
  ○ Won **1st place** in the WMT22 competition by achieving the best BLEU 14.09 and ChrF++ 37.42 [code]
  ○ Preprocessed large-scale (10 million) African language corpus
  ○ Optimized the system to mitigate the data imbalanced issue, achieving 21.55% improvement

Work Experiences

- **Agriculture IoT System** Shenzhen, China
  Advisor: Prof. Yeh-Ching Chung, CUHK | Co-founder, AgriFuture *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

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

Skills

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