HAIZHONG ZHENG

Ph.D. candidate, University of Michigan, Ann Arbor
http://zhenghaizhong.com/ Email: hzzheng@umich.edu;

RESEARCH INTERESTS

Efficient machine learning; Machine learning data efficiency; LLM inference efficiency; ML security and privacy.

EDUCATION & EXPERIENCE

Ph.D. Candidate in Computer Science and Engineering — Sep 2018 - Present
University of Michigan, Ann Arbor, MI, USA

M.S. in Computer Science and Technology — Sep. 2015 - Mar. 2018
Shanghai Jiao Tong University (SJTU), Shanghai, China

B.S. in Computer Science and Technology — Sep. 2011 - June 2015
Shanghai Jiao Tong University (SJTU), Shanghai, China

WORK EXPERIENCE

Applied Scientist Intern, Amazon Web Service, Seattle, WA — May. 2021 - Aug. 2021
Mentored by Dr. Wei Zhang and Dr. Qian Cui in Security Analytics and AI Research (SAAR) team.
Anomaly detection with time series forecasting for AWS GuardDuty intelligent threat detection system.

Research Intern, Lawrence Livermore National Laboratory (LLNL), Livermore, CA — May. 2023 - Aug. 2023
Mentored by Dr. Bhavya Kailkhura.
Improve LLM inference efficiency.

GRANT PROPOSAL

I actively contributed to the proposal writing and presentation for the following grants:

Data efficiency of LLMs fine-tuning with RLHF	150*K per year*, Cisico, 2023
Intelligent Assistants for Detecting Social Engineering Scams	100*K*, OpenAI, 2023

SELECTED PUBLICATIONS

PREPRINT

[*P*2] Learn To be Efficient: Build Structured Sparsity in Large Language Models, Preprint
Haizhong Zheng, Xiaoyan Bai, Beidi Chen, Fan Lai, Atul Prakash

[*P*1] Leveraging Hierarchical Feature Sharing for Efficient Dataset Condensation, Preprint
Haizhong Zheng, Jiachen Sun, Shutong Wu, Bhavya Kailkhura, Zhuoqing Mao, Chaowei Xiao, Atul Prakash

CONFERENCE

[C4] CALICO: Self-Supervised Camera-LiDAR Contrastive Pre-training for BEV Perception, ***ICLR*** 2024
Jiachen Sun, **Haizhong Zheng**, Qingzhao Zhang, Atul Prakash, Z. Morley Mao, Chaowei Xiao

[C3] Coverage-centric Coreset Selection for High Pruning Rates, ***ICLR*** 2023
Haizhong Zheng, Rui Liu, Fan Lai, Atul Prakash

[C2] Efficient Adversarial Training with Transferable Adversarial Examples, ***CVPR*** 2020
Haizhong Zheng, Ziqi Zhang, Juncheng Gu, Honglak Lee, Atul Prakash

[C1] Smoke Screener or Straight Shooter: Detecting Elite Sybil Attacks in User-Review Social Networks, ***NDSS*** 2018
Haizhong Zheng, Minhui Xue, Hao Lu, Shuang Hao, Haojin Zhu, Xiaohui Liang, Keith Ross

WORKSHOP

[*W*1] Analyzing the Interpretability Robustness of Self-Explaining Models, ***ICML'***19 Workshop on the Security and Privacy of Machine Learning
Haizhong Zheng, Earlence Fernandes, Atul Prakash

Teaching Experience

Co-Lead Instructor, Secure and Trustworthy Machine Learning (UMich EECS 598) 2023 Winter

EECS 598 covers research topics in machine learning security and privacy. My responsibility is to design the course, teach the lectures, lead discussions, and advise course projects.

Graduate Student Instructor, Data Structures and Algorithms (UMich EECS 281) 2021 Fall

EECS 281 is a well-organized course with over 1000 students each term. My responsibility is to give lectures and leading discussions on a weekly lab section and hold 6hrs office hours for each week.

Academic Service

Conference/Journal Paper Reviewer: ECCV 2020, TPAMI 2020, ICLR 2022, NeurIPS 2022, ICLR 2023, ICML 2023, NeurIPS 2023, AAAI 2024, ICLR 2024

Honors and Awards

Rackham Travel Grant: ICML'19	2019
Academic Excellence Scholarship of Shanghai Jiao Tong University	2015-2017
Second Prize in the Twelfth China Post-Graduate Mathematical Contest in Modeling	2016
Best Presentation Award in A3 Foresight Program 2015 Annual Workshop	2015
Academic Excellence Scholarship of Shanghai Jiao Tong University	2012-2014
National Olympiad in Informatics in Provinces (NOIP), First Prize	2010

Last updated: 2024.2