Zain Sarwar

309-703-5234 | zsarwar@uchicago.edu | linkedin.com/in/zainsarwar865 | zainsarwar865.github.io | Google Scholar

RESEARCH INTERESTS

Designing efficient architectures for NLP, Retrieval Augmented LLMs, Sparse computation in deep models, Pre-training strategies for LLMs & Safety for Generative AI

EDUCATION

University of Chicago Chicago, IL
PhD in Computer Science Aug 2025 (Expected)
GPA: 3.91/4.0
Relevant Coursework: Deep Learning, Machine Learning, Operating Systems, NLP, Algorithms & Distributed systems

Lahore University of Management Sciences (LUMS) Lahore, Pakistan
BSc in Computer Science & Economics May 2020
GPA: 3.79/4.0
Honors: Dean's Honor List

PROFESSIONAL EXPERIENCE

University of Chicago Chicago, IL
Research Assistant *September 2021 – Present*

- Developed an algorithm for improving image classification models which finds gaps in the training data and fills them by finding the most useful data in external datasets using supervised and unsupervised algorithms. This algorithm can be used to value large-scale private datasets in data markets
- Invented a first-of-its-kind safety analysis tool for LLMs which can detect the model's tendency to hallucinate sensitive information by crafting semantically meaningful prompts using a retrieval mechanism
- Engineered state-of-the-art techniques for detecting text generated from Large Language models using graph neural networks that can be used to detect LLM generated fake news, hate speech etc.
- Created a voice privacy protection tool which prevents deep learning models from cloning an individual's voice to protect against identity theft using a voice anonymizing neural model
- Implemented the first ever end-to-end generalizable video and virtual reality based keystroke inference attack which uses a novel self-supervised learning algorithm to connect classical machine learning with deep neural networks and has applications in VR and hand tracking systems

PosterMyWall Lahore, Pakistan
Software Engineer *May 2020 - Oct 2020*

- Formulated a new SEO strategy to adapt to search engines using machine learning for site ranking
- Fixed critical site issues which decreased website bounce rate by 4% and improved click-through rate by 7%
- Automated data analysis related to keyword optimization which eliminated 20+ hours of monthly research

PUBLICATIONS

Can Virtual Reality Protect Users from Keystroke Inference Attacks?
Zhuolin Yang, **Zain Sarwar**, Iris Hwang, Ronik Bhaskar, Ben Y. Zhao, Haitao Zheng
USENIX Security Philadelphia, PA, August 2024.

Deepfake Text Detection: Limitations and Opportunities
Jiameng Pu, **Zain Sarwar**, Sifat Muhammad Abdullah, Abdullah Rehman, Mobin Javed, and Bimal Viswanath
IEEE S&P (Oakland) 2023

Towards a General Video-based Keystroke Inference Attack
Zhuolin Yang, Yuxin Chen, **Zain Sarwar**, Hadleigh Schwartz, Ben Y. Zhao, Haitao Zheng
USENIX Security Anaheim CA, August 2023

TECHNICAL SKILLS

Languages: Python, C, C++, Java, JavaScript, Go, Haskell, Matlab, SQL
Libraries: PyTorch, TensorFlow, OpenCV, scikit-learn, pandas, NumPy, Selenium
Frameworks: Angular, React, Git, Docker, Flask, Node.js, Vue