Mujahid Al Rafi

Resume

✉ *mrafi@ucmerced.edu*
LinkedIn

Education

PhD Student	**University of California, Merced**, CA, USA 2021 – Present, Electrical Engineering and Computer Science Anticipated Graduation Date: May 2026 MoCA Lab (link) Advisor: Prof. Hyeran Jeon.
Bachelor of Science	**Bangladesh University of Engineering and Technology**, Dhaka, Bangladesh 2013 - 2018, Computer Science and Engineering .

Research Interests

- Computer Architecture
- GPU Security and Reliability
- Secure DNN Computing

Publications and Presentations

IISWC 2023	**Decepticon: Attacking Secrets of Transformers** Mujahid Al Rafi, Yuan Feng, Fan Yao, Meng Tang, Hyeran Jeon
NOPE'22, ASPLOS Workshop	**Too Noisy To Extract: Pitfalls of Model Extraction Attacks** Mujahid Al Rafi, Yuan Feng, Hyeran Jeon

Research and Work Experience

Graduate Student Researcher	University of California, Merced, CA, USA Aug. 2021 - Present Mentor: Prof. Hyeran Jeon
Program Committee Member	The 50th International Symposium on Computer Architecture Artifact Evaluation (ISCA 2023 AE)
Software Engineer	CodeCrafters International, Dhaka, Bangladesh Jan. 2018 - Jul. 2021 Mentor: Ellis Miller I was part of a C++ development team providing core development on a 1.5 million LOC software project used by Fortune 500 companies.

Research Projects

Model Extraction Attacks on Transformers

In this project, we explored the security impact of using publicly-accessible pre-trained Transformer models. We showed, through a novel model extraction attack, that the pre-trained model of a black-box fine-tuned model can be identified by using model fingerprints. We leveraged the weight value similarity between a pretrained and its finetuned models to extract the weights of the victim model. The extracted model shows almost alike prediction accuracy with over 94% matching prediction outputs with the victim model.

GDDR Row Hammering

In this project, we are exploring the row hammer attack on GDDR memory widely used in GPUs.

Better Utilize Tensor Cores

In this project, we are exploring efficient offloading of work from CUDA cores to Tensor cores.

Selected Professional Projects

2020 **Archive Unused Files**

In this project, I enabled our system-update to archive unused and unchanged (for a specific period) files to a specific location from where they can be restored later if necessary. Activity log and metadata were used to make the decision whether a file or any of its dependant files was recently used or modified. Breadth-first search was used to explore the dependency-related files. Clients appreciated the cleaner file storage after using this feature.

2019 **Import Engine Enhancement**

In this project, I enhanced our data import engine to import data from various types of files like txt, csv, PDF, XLSX, XLS etc. Made our import command line interface smart enough to infer data delimiter from the import file extension.

2019 **Report Engine Enhancement**

In this project, I enhanced our report rendering engine to conditionally show or hide group of data based on the sorting column. I also made the column sort order (ascending-first or descending-first) more intuitive based on the column data type.

2018 **Speedup File Search**

Our file search tool was reported to be too slow. I profiled the search procedure and found the file usage filter as the main bottleneck. Communicating with the clients revealed that they seldom use this filter. So we ended up making this file usage filter optional and turned off by default. The speedup was as high as 60% in systems having lots of usage data.

Teaching Experience

Teaching Assistant **CSE, University of California, Merced**

- CSE 140: Computer Architecture (Spring 2022)
- CSE 165: Introduction to Object Orientated Programming (Fall 2022)

- CSE 030: Data Structures (Spring 2023)

Awards

2022 and 2023	EECS Bobcat Fellowship

Computer Skills

Programming	C/C++, Python
Database	SQL, Oracle
Others	PyTorch, CUDA, LaTeX