AHMAD FARAZ KHAN

ahmadfk@vt.edu | afkd98.github.io

EDUCATION

Ph.D. in Computer Science, Virginia Tech, Blacksburg, VA (**CGPA 3.8**) *December 2020 - Present*
Research Focus: Machine Learning Systems

B.S. in Computer Science, LUMS, Lahore, Pakistan *2016-2020*
Advanced Courses: Distributed Systems, Deep Learning, Machine Learning, Cloud Development, Computer Systems

TECHNICAL PROFICIENCY

Programming Languages: Python, Javascript, C/C++, Java, Go.
Tools, Libraries: Pytorch, Tensorflow, PySpark, AWS Suite, Dask, Numba, Hadoop, Docker, Kubernetes, OpenFaaS, Selenium, MongoDB, ES6+, TypeScript, React, Node, Express, SQL, CUDA

PUBLICATIONS

Graduate Research Assistant, DSSL, Virginia Tech December 2020 - Present
Mentor: Dr. Ali Butt, PhD. Purdue University

– Designed ”FLStore” cache for handling non-training workloads of FL efficiently at low cost. Submitted to **ACM EuroSys'25**.

– Designed ”FLOAT”, a framework optimizing Federated Learning's resource utilization and model performance amid heterogeneity, leveraging Reinforcement Learning with Human Feedback. Published in **ACM EuroSys'24**.

– Analyzed personalized FL algorithms, revealing trade-offs between privacy, efficiency, and performance. Paper submitted to **VLDB'24**.

– Designed an incentive-driven personalized FL framework for statistical heterogeneity. Paper submitted to **NeurIPS'24**.

– Developed a Direct Preference Optimization approach harnessing human preferences for prompt optimization of text-to-image tasks. Submitted to **COLM'24**.

– Introduced a Direct Preference Optimization approach to mitigate sycophancy by fine-tuning LLMs on a curated dataset. Submitted to **ICML Workshop'24**.

– Designed an adaptive FL aggregator for Edge and IoT, achieving 4× scalability, 8× time efficiency, and 2× cost savings over conventional methods. Published in **IEEE BigData'23**.

– Conducted a survey on adversarial tactics in DNN, DRL, FL, and TL deep learning models, emphasizing their applications and distinct features. Published in **IEEE Access'24**.

– Monetized VFL with `PERFACY-FL`, an incentive mechanism valuing data quality and privacy using Homomorphic Encryption, boosting participation and profitability. Paper under review.

– Designed and developed an incentivize system for FL on the IBMfl lib. Paper published in **FL-AAAI'22, IEEE CLOUD'22**.

– Designed a heterogeneity-aware adaptive FL scheduling system to tune (1) accuracy, (2) resource and accuracy fairness, and (3) training time of the model according to user preferences using IBMfl lib. Paper published in **IEEE BigData'22**.

Research Assistant, Networks and Systems Group, LUMS January 2019 - May 2020
Mentor: Dr. Ihsan Ayyub Qazi, PhD. University of Pittsburgh

– Created a data-driven video streaming algorithm (DAVS), realizing a 20% QoE enhancement over the state-of-the-art ABR algorithm Pensieve.

KEY PROJECTS

ML System Optimization: Pioneered algorithms to enhance the architecture of ML systems, targeting resource allocation, scalability, and cost-time efficiency. This work culminated in the research papers published and submitted to (IEEE CLOUD'22, BigData'22, BigData'23, EuroSys'24).

Federated Learning Frameworks: Spearheaded the design and development of both Horizontal and Vertical Federated Learning (HFL & VFL) frameworks. Furthermore, implemented MLOps pipelines integrated with AWS cloud resources and popular ML libraries such as PyTorch, TensorFlow, and FedScale (AAAI'24, AAMAS'24).

Designed a distributed and containerized system with a dynamic pipeline to support the data analytical modules for Cyber Infrastructure for Waterborne Antibiotic Resistance Risk Surveillance (CI4-WARS).

Counter Fuzzing with LLVM: Developed an LLVM-based counter fuzzing approach that's undetectable by leading fuzzers like AFL and balances performance with countermeasures.

SERVICES

- Served on the external review committee for USENIX ATC 2024.

- Reviewed for Neural Processing Letters 2022 & 2023.

ADDITIONAL EXPERIENCES

Teaching Roles, Virginia Tech: Instructed courses such as Web/Cloud Development (Summer'24 & Fall'23), Python Programming (Spring'20, Fall'21), and Principles of Computer Security (Spring'22).

Associate Data Engineer, i2c Inc. (May 2020 - December 2020): Spearheaded the development and upkeep of distributed sequential databases. Successfully accelerated query times for read-only tasks through database optimization techniques.