AHMAD FARAZ KHAN

ahmadfk@vt.edu | afkd98.github.io

EDUCATION

Ph.D. in Computer Science, Virginia Tech, Blacksburg, VA *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

- Ahmad Faraz Khan, Samuel Fountain, Ahmed M. Abdelmoniem, Ali R. Butt, and Ali Anwar. FLStore: Federated Learning Optimizations with Automated Tuning. Under Review at the 20th ACM European Conference on Computer Systems **(EuroSys'25)**.
- Ahmad Faraz Khan, Azal Ahmad Khan, Ahmed M. Abdelmoniem, Samuel Fountain, Ali R. Butt, and Ali Anwar. FLOAT: Federated Learning Optimizations with Automated Tuning. In Proceedings of the 19th ACM European Conference on Computer Systems **(EuroSys'24)**, Athens, Greece, 12 pages, April 2024. (AR: 16%).
- Ahmad Faraz Khan, Xinran Wang, Qi Le, Zain ul Abdeen, Azal Ahmad Khan, Haider Ali, Ming Jin, Jie Ding, Ali R. Butt, and Ali Anwar. IP-FL: Incentive-driven Personalization in Federated Learning. Under Review at the 38th Annual Conference on Neural Information Processing Systems **(NeurIPS'24)**.
- Azal Ahmad Khan, Xinran Wang, Ahmad Faraz Khan, Ali Anwar, and Debanga Raj Neog. Direct Preference Optimization for Prompt Engineering in Text-to-Image Synthesis. Under Review at the 1st Conference on Language Modeling **(COLM'24)**.
- Azal Ahmad Khan, Sayan Alam, Xinran Wang, Ahmad Faraz Khan, Ali Anwar, and Debanga Raj Neog. Mitigating Sycophancy in Large Language Models via Direct Preference Optimization. Under Review at ICML 2024 ICML Workshop on Models of Human Feedback for AI Alignment **(ICML Workshop'24)**.
- Haider Ali, Ahmad Faraz Khan, Sindhuja Madabushi, Ananthram Swami, Rui Ning, Hongyi Wu, and Jin-Hee Cho. PETER: Privacy-Preserving Vertical Federated Learning Against Feature Inference Attacks. Under Review at the IEEE Transactions on Information Forensics and Security **(TIFS'24)**.
- Sindhuja Madabushi, Ahmad Faraz Khan, Haider Ali, and Jin-Hee Cho. Privacy Preserving and Feature Importance Based Incentive Mechanism in Vertical Federated Learning. To be submitted to the 39th Annual AAAI Conference on Artificial Intelligence **(AAAI'25)**.
- Xinran Wang, Qi Le, Ahmad Khan, Jie Ding and Ali Anwar. ICL: Generic Framework for Incentivized Collaborative Learning. Under Review at the 7th AAAI Conference on AI, Ethics, and Society **(AAAI-AIES'24)**.
- Ahmad Khan, Yuze Li, Xinran Wang, Sabaat Haroon, Haider Ali, Yue Cheng, Ali R. Butt, and Ali Anwar. Towards Cost-Effective and Resource-Aware Aggregation at Edge for Federated Learning. In Proceedings of the 2023 IEEE International Conference on Big Data **(BigData'23)**, Sorrento, Italy, 10 pages, December 2023. (AR: 17.49%).
- Haider Ali, Dian Chen, Matthew Harrington, Nathaniel Salazar, Mohannad Al Ameedi, Ahmad Faraz Khan, Ali R. Butt, and Jin-Hee Cho. A Survey on Attacks and Their Countermeasures in Deep Learning: Applications

in Deep Neural Networks, Federated, Transfer, and Deep Reinforcement Learning. In **IEEE Access**: The Multidisciplinary Open Access Journal, vol. 11, pp. 120095-120130, October 2023. (AR: 30%).

- Jingoo Han, Ahmad Faraz Khan, Syed Zawad, Ali Anwar, Nathalie Baracaldo Angel, Yi Zhou, Feng Yan, and Ali R. Butt. TIFF: Tokenized Incentive for Federated Learning. In Proceedings of the IEEE International Conference on Cloud Computing **(CLOUD'22)**, Barcelona, Spain, 10 pages, July 2022. (AR: 22.4%).
- Jingoo Han, Ahmad Faraz Khan, Syed Zawad, Ali Anwar, Nathalie Baracaldo Angel, Yi Zhou, Feng Yan, and Ali R. Butt. Heterogeneity-Aware Adaptive Federated Learning Scheduling. In Proceedings of the IEEE International Conference on Big Data **(BigData'22)**, Osaka, Japan, 10 pages, December 2022. (AR: 19.2%).
- Jingoo Han, Ahmad Faraz Khan, Syed Zawad, Ali Anwar, Nathalie Baracaldo Angel, Yi Zhou, Feng Yan, and Ali R. Butt. Tokenized Incentive for Federated Learning. In Proceedings of the AAAI International Workshop on Trustable, Verifiable and Auditable Federated Learning **(FL-AAAI-22)** in conjunction with AAAI 2022, Vancouver, BC, Canada, 9 pages, March 2022.

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

Systems for ML: Optimized state-of-the-art distributed learning systems, focusing on enhancing resource utilization, scalability, and efficiency through the development of specialized computing and storage solutions for resource-constrained environments. This research led to papers that were published and presented at conferences including BigData'22, BigData'23, and EuroSys'24, and submissions in EuroSys'25.

Privacy-aware Learning: Designed and developed Horizontal and Vertical Federated Learning (HFL & VFL) frameworks, enhancing privacy in distributed environments. In addition, implemented MLOps pipelines that leverage cloud resources and integrate with major ML libraries such as PyTorch, TensorFlow, and FLOWER. This work contributed to publications at IEEE Access'23, and the FL-AAAI'22.

Personalized ML: Developed enhanced personalization solutions for resource-constrained distributed ML systems, aiming to tailor models more effectively to individual user needs. This work led to contributions under review at NeurIPS'24, AAAI

Incentivized ML: Improved incentive mechanisms within distributed and collaborative resource-constrained ML systems to ensure fairness and adaptability across diverse user groups and scenarios. This work led to contributions towards IEEE CLOUD'22, AAAI-AIES'24, and AAAI'25.

LLMs fine-tuning: Developed a Direct Preference Optimization (DPO) approach that utilizes human preferences for rapid optimization of text-to-image tasks. Furthermore, introduced a DPO method to reduce sycophancy by fine-tuning large language models (LLMs) using a curated dataset. These contributions are under review at COLM'24 and ICML Workshop'24.

DevOps: 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).

Program Analysis: Developed an LLVM-based counter fuzzing approach that's undetectable by leading fuzzers such as 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.