Website
Google Scholar

# MOMIN AHMAD KHAN

makhan@umass.edu

## INTERESTS

**Security and Privacy of Distributed Machine Learning Systems**

## EDUCATION

**Amherst, MA** | **University of Massachusetts Amherst** | **Sep 2021 – Present**

- PhD in Electrical and Computer Engineering, GPA: 3.95/4.0.

**Islamabad, Pakistan** | **National University of Sciences and Technology** | **2017 - 2021**

- Bachelor's in Electrical Engineering, GPA: 4.0/4.0.

## PUBLICATIONS

- **HYDRA-FL: Hybrid Knowledge Distillation for Robust and Accurate Federated Learning [paper]**
  **Momin Ahmad Khan**, Yasra Chandio, Fatima Muhammad Anwar
  *38th Conference on Neural Information Processing Systems (NeurIPS 2024).*
- **Decoding FL Defenses: Systemization, Pitfalls, and Remedies**
  **Momin Ahmad Khan**, Virat Shejwalkar, Amir Houmansadr, Fatima Muhammad Anwar
  **(Under Review)**
- **A Neurosymbolic Approach to Adaptive Feature Extraction in SLAM [paper]**
  Yasra Chandio, **Momin Ahmad Khan**, Khotso Selialia, Joseph Degol, Luis Garcia, Fatima Anwar
  *IEEE/RSJ International Conference on Intelligent Robots and Systems (**IROS**), 2024*
- **On the Pitfalls of Security Evaluation of Robust Federated Learning [paper]**
  **Momin Ahmad Khan**, Virat Shejwalkar, Amir Houmansadr, Fatima Muhammad Anwar
  *6th Deep Learning Security and Privacy Workshop at IEEE Security and Privacy, 2023*
- **Security Analysis of SplitFed Learning [paper]**
  **Momin Ahmad Khan**, Virat Shejwalkar, Amir Houmansadr, Fatima Muhammad Anwar
  *SenSys Workshop on Challenges in AI and ML for IoT **(SenSys AIChallengeIoT), 2022***
- **Universal Timestamping with Ambient Sensing [paper]**
  Adeel Nasrullah, **Momin Ahmad Khan**, Fatima Muhammar Anwar
  *19th Annual IEEE International Conference on Sensing, Communication, and Networking (**SECON**), 2022*

## WORK EXPERIENCE

**Research Intern** | **Nokia Bell Labs, Murray Hill, NJ** | **Jun 2024 – Aug 2024**

- Manager: Manzoor Khan
- Created the model selection pipeline for a Bell Labs internal system. Used LLM agents and tools to create an autonomous system for data curation and optimal model selection.
- Designed a smart multimodal meeting assistant for Bell Labs, powered by different LLMs, computer vision modules, and hardware components to replace a human meeting manager.

**Research Assistant** | **University of Massachusetts Amherst** | **Sep 2021 - Present**

- Advisor: Professor Fatima Anwar
- Identified 6 distinct pitfalls in Federated Learning Robustness evaluations after thoroughly surveying 50 top-tier papers, performed an impact analysis for each pitfall using case studies, and provided actionable recommendations for each of them.

**Research Assistant** | **SIGMA Lab, NUST Islamabad** | **Jun 2019 – May 2021**

- Advisor: Imran Abeel. Co-Advisors: Faisal Shafait & Hassan Aqeel Khan
- Engineered a low-cost Whole-slide Imaging Scanner for automating slide digitization and integrated it with deep-learning for accurate cancer cell detection.

- Mentored summer interns in 2020, offering easy-to-implement projects for hands-on deep learning expertise.

| | | |
|---|---|---|
| **Research Assistant** | **TUKL Lab, NUST Islamabad** | **Oct 2020 – May 2021** |

- Optimized deep learning acceleration using TensorRT for NVIDIA Jetson devices to boost Jetson Nano's inference speed by 3.5x.

| | | |
|---|---|---|
| **Teaching Assistant** | **AI-Lounge** | **Jun 2020 – May 2021** |

- Created tailored course content on deep learning and computer vision for school children. Simplified complex topics using intuitive methods and engaging visuals.

| | | |
|---|---|---|
| **Community Service Intern** | **Akhuwat Foundation** | **Jun 2018 – Jul 2018** |

- Conducted door-to-door collections in addition to clothes collection camps, gathering donations for distribution. Ensured effective delivery to deserving individuals, supporting multiple deserving communities.

## INDUSTRIAL PROJECTS

**Mobile Datalogger for Testbed-scale Car.**

| | |
|---|---|
| NUST and Sedenius Technologies | **Aug 2020 – Sep 2020** |

**PCB Design for Arduino and Odroid Connectivity of an Autonomous Car**

| | |
|---|---|
| NUST and Sedenius Technologies | **Oct 2020 – Nov 2020** |

## AWARDS AND ACHIEVEMENTS

- Rector's Gold Medal for best Final Year Project, NUST, 2021
- Chancellor's Silver Medal for academic performance, NUST, 2021
- Recipient of merit scholarship at NUST (2017-2021)
- 1st Position in PIEAS Entrance Examination 2017
- 1st Position in GIKI Entrance Examination 2017
- 13th Position in NUST Entrance Examination 2017

## TECHNICAL SKILLS

- Programming Language: Python, C++, MATLAB
- Machine Learning Tools & Frameworks(s): PyTorch, FedJAX, Keras, Langchain