Syed Moiz Ali

+1 872 (265) 8628 | moizsyedali.ma@gmail.com | linkedin.com/in/moizali01 | github.com/moizali01

Education

University of Illinois at Chicago — Chicago, IL
Ph.D. in Computer Science — *Sep. 2025 – Present*

Lahore University of Management Sciences — Lahore, Pakistan
Bachelor of Science in Computer Science — *Sep. 2021 – May 2025*

Relevant Coursework: Topics in Computer and Network Security, Deep Learning, Machine Learning, Network Security, Topics in Large Language Models, Computer Vision, Probability, Algorithms

Work Experience

Generative AI Engineer — June 2025 – Aug 2025
Technology for People Initiative (TPI), LUMS — *Lahore, Pakistan*

- Developed a LangChain based multiagent AI tax lawyer to automatically analyze tax notices and generate tailored compliance responses, streamlining regulatory processes and reducing manual processing overhead.
- Designed and implemented scalable refine chain pipelines with complexity-based routing, enabling differentiated processing paths for consumer vs. enterprise tax scenarios.
- Built automated document parsing and contextual response generation capabilities, improving compliance accuracy and significantly reducing manual review requirements.

Research Assistant — Feb 2024 – May 2025
Security & Privacy Lab, LUMS — *Lahore, Pakistan*

- Collaborated with Stanford Research Institute, University of Arizona, and Google to develop a novel RAG-based multiagent LLM pipeline that assists traditional debloaters by retaining code critical for functionality and generality. Achieved improved generality and stability across benchmarks when integrated with three existing debloaters, with minimal size impact.
- Evaluated how fine-tuned LLMs internalize and transfer knowledge new across surface-level and deep comprehension tasks, analyzing the role of model size and task complexity in generalization. Accepted to **EMNLP Findings 2025**.
- Investigated task-specific safety degradation in finetuning of LLMs, uncovering vulnerabilities in tasks such as code generation, translation, and classification. Developed and curated MultitaskBench a safety alignment dataset that enhances safety across various LLM tasks. Published at **COLING 2025**.
- Designed a probabilistic framework to detect hallucinations, analyzing log probabilities and top-k token distributions. Conducted initial benchmarks to identify patterns distinguishing confident and hallucinated responses.

Projects

Tradesnap.ai | *MERN, Selenium, Azure Cloud, OpenAI* — Jan 2024 – May 2024

- Developed a conversational stock trading platform using OpenAI's Assistant to enable multilingual stock trading via chat interface.
- Integrated features like buying/selling stocks, educational content, and personalized volatility alerts.
- Scraped data from PSX for platform backend and built detailed company pages with advanced React charts.
- Implemented automated testing for the application using Selenium to ensure platform reliability.

Nighttime Wildlife Monitoring | *CycleGAN, Image Processing, OpenAI CLIP* — Jan 2024 – May 2024

- Developed a hierarchical model leveraging CycleGANs to enhance nighttime camera trap images for snow leopard detection.
- Used OpenAI's CLIP for image classification and fine-tuned it for challenging nighttime conditions.
- Collected and curated training data from the Snapshot Serengeti Database, achieving 0.95 accuracy and 0.89 F1-score.

Urban Electricity Analytics | *Selenium, LSTM, Python, Pandas* — Jun 2023 – Aug 2023

- Developed a high-performance web scraper using **Selenium** and multithreading to extract electricity consumption data for over 3 million users across Lahore.

- Engineered an **LSTM**-based time series forecasting model to predict feeder overloading, improving grid management strategies.
- Conducted analysis of seasonal consumption patterns to identify **poverty hotspots**.

Social Media Toxicity Classifier | *Llama2, PEFT, Jigsaw Dataset* Jan 2024 – May 2024

- Developed a model to detect and flag harmful social media content, fine-tuning Llama2-7B (PEFT) for toxicity classification.
- Achieved 90% accuracy and an F1-score of 0.89 across 6 toxic classes using the Jigsaw Toxic Comment Classification Dataset.
- Reached a ROC of 0.85, ensuring effective detection of harmful content.

Publications

MultitaskBench: Unveiling and Mitigating Safety Gaps in LLMs Fine-tuning | *arXiv:2409.15361* 2025

- Essa Jan, Nouar AlDahoul, **Moiz Ali**, Faizan Ahmad, Fareed Zaffar, Yasir Zaki.
- Investigates task-specific safety gaps in fine-tuned LLMs and proposes a multitask safety dataset to mitigate them.
- Published at **COLING 2025**.

Data Doping or True Intelligence? Evaluating the Transferability of Injected Knowledge in LLMs | *arXiv:2505.17140* 2025

- Essa Jan, **Moiz Ali**, Saram Hassan, Fareed Zaffar, Yasir Zaki.
- Studies how supervised fine-tuning affects the generalization of injected knowledge across tasks with diverse formats and objectives.
- Accepted to **EMNLP Findings 2025.**

Teaching Experience

Graduate Teaching Assistant Aug 2025 - Dec 2025

University of Illinois at Chicago

- CS107: Introduction to Computing and Programming (Fall 2025, Dr. Jason Polakis).

Undergraduate Teaching Assistant Sep 2023 – May 2025

Lahore University of Management Sciences

- CS100: Computational Problem Solving (Spring 2025, Dr. Fareed Zaffar).
- CS437: Computer Vision Fundamentals (Fall 2024, Dr. Murtaza Taj).
- CS100: Computational Problem Solving (Spring 2024, Dr. Fareed Zaffar).
- CS200: Introduction to Programming (Fall 2023, Dr. Shafay Shamail).

Technical Skills

Languages: Python, JavaScript, C, C++, Haskell, HTML, CSS, Bash
Technologies/Frameworks: PyTorch, TensorFlow, OpenCV, MERN, TypeScript, LLVM, LangChain, Pandas, Scikit-learn, LlamaIndex, OpenAI Platform, Google AI Studio, Selenium, Azure Cloud