

# MUHAMMAD ABUBAKAR MUGHAL

26100228@lums.edu.pk | LinkedIn/m-a-mughal | GitHub/AbubakarMughal1 | Kaggle/mabubakarmughal

## EDUCATION

|  |   |
|--|---|
| <b>Lahore University of Management Sciences</b><br><i>Bachelors of Science in Computer Science; Major GPA: 3.66/4.00</i> | Sep 2022 – Jun 2026<br>Lahore, Pakistan |
| <b>Relevant Coursework:</b> Distributed Systems, Topics in Large Language Models, Deep Learning, Computer Architecture   |   |

## PUBLICATIONS

### The Synthetic Stream: Prevalence and Engagement with AI Content on YouTube

Muhammad Muiz Farhan\*, Muhammad Abubakar Mughal\*, Ihsan Ayyub Qazi, Zafar Ayyub Qazi (*Under review in ACM Web Conference 2026*) \*Equal contributions.

## RESEARCH EXPERIENCE

|   |  |
|---|--|
| <b>Research Assistant</b><br><i>Distributed &amp; AI Systems Lab @ LUMS</i> | Jan 2025 – Present<br>Lahore, Pakistan |
|---|--|

#### *Project: Large-Scale Analysis of AI-Generated Content and Recommendation Patterns on YouTube*

- Collected a global dataset of 1.13M+ trending videos on YouTube, and 220k+ recommendations using the YouTube Data API and custom Selenium scripts.
- Built statistical and regression analysis scripts showing that 11.6% of the content was AI-tagged, and these gained 10.2% more views but 46.7% fewer likes. Temporal regression highlighted a ~ 2.1% increase in prevalence of AI-tagged videos over the data collection period.
- Implemented a Selenium crawler to map YouTube's recommendation graph, finding that viewing one AI-tagged video raised the probability of subsequent AI exposure by 51% and sustained this pattern for an average of 13.7 hops.
- Led a 60 participant study to measure how literacy levels affect the detection of AI-generated videos, showing that low-literacy users identified only 42% correctly while high-literacy users reached 77%.

#### *Project: Security Evaluation of Agentic Browsers under Injection-Based Attacks (collaboration with SANDs Lab @ KAUST)*

- Analyzing how agentic browsers respond to prompt-injections and jailbreak attacks by running controlled attack scenarios through web-pages on major social media platforms, analyzing agent vulnerabilities and behavior as well as evaluating platform-level guardrails and mitigation systems.
- Designing an experimental framework to evaluate DOM-aware browser agents (e.g., Perplexity Comet), across 4 direct injection strategies, measuring where and how their defenses fail.
- Validating the framework by deploying controlled attack vectors inside sand-boxed social-media workflows and capturing how agentic browsers behave under full end-to-end adversarial conditions.
- Preparing a manuscript that systematizes the empirical results, formalizes the threat model and presents the evaluation framework for submission to a peer-reviewed security venue.

## TEACHING EXPERIENCE

|   |                             |
|---|-----------------------------|
| <b>Teaching Assistant, CS382: Network Centric Computing</b> | Jan 2025 - May 2025<br>LUMS |
|---|-----------------------------|

- Supported ~ 180 students through biweekly office hours, debugging guidance, and programming help.
- Delivered live and recorded tutorials, produced practice sets, and managed the course Slack channel.

|   |                             |
|---|-----------------------------|
| <b>Teaching Assistant, CS200: Object Oriented Programming</b> | Sep 2024 - Dec 2024<br>LUMS |
|---|-----------------------------|

- Assisted ~ 130 students via biweekly office hours, led and invigilated weekly lab sessions and handled course communication and Q&A on Slack.

## PROFESSIONAL EXPERIENCE

---

### Development Intern

Jul 2025 – Aug 2025

*TechLogix – IT Services and Enterprise Software Consultants*

- Evaluated a proposed OCR pipeline for Protected Health Information extraction across 24 configurations of medical devices and tests, assessing technical viability and HIPAA compliance requirements.
- Assessed 2 deployment configurations across Azure OpenAI Services and Azure Document Intelligence to identify a secure, feasible rollout path, producing a framework proposal for the client.

### FrontEnd Development Intern

Jun 2023 - Aug 2023

*RolusTech – CRM and Cloud Solutions Partner*

- Built responsive HTML/CSS pages from Figma specs in close coordination with the team designer, ensuring accurate implementation of layouts and components.

## DEVELOPMENT PROJECTS

---

### Distributed Key-Value Store with Raft-Based Fault Tolerance | Go

- Implemented the Raft consensus protocol in Go, enabling leader election, log replication, and strong consistency for a distributed key-value store built from scratch.
- Added durable log persistence and coordinated state-machine execution across nodes to achieve fault-tolerant recovery and stable operation under node failures.

### Document Retrieval and QA Pipeline (RAG) | Python, Langchain, HuggingFace

- Built a RAG system that answers queries over PDF/Word/text documents using BGE-small embeddings and a local vector store.
- Added duplicate-document detection in ChromaDB and adaptive chunking that sizes text segments by document complexity, improving retrieval precision and reducing irrelevant hits.
- Designed a modular LangChain pipeline with a Streamlit UI that allows swapping LLMs and embedding models without code changes.

### Solar Panel Detection on Low-Res Satellite Imagery | Python, YOLO, QGIS, OpenCV

- Built a two-stage, fine-tuned YOLO pipeline to detect solar panels in low-resolution satellite imagery.
- Curated and manually annotated ~ 330 satellite images of Lahore, Pakistan in QGIS/OpenCV to create a bounding-box dataset tailored for the task.
- Improved detection accuracy by pre-processing test images with SwinIR and SinSR super-resolution models to restore spatial and textural detail.

### Web Application Security Hardening | Python, FastAPI

- Implemented OAuth 2.0 authentication with JWT validation and RBAC in a FastAPI application.
- Exercised CSRF and XSS vectors in controlled scenarios to break transaction integrity and seize active user sessions.
- Applied CSRF tokens, SameSite cookies and input sanitization to eliminate the attack paths and restore secure request handling.

### LUMScape: Interactive 3D Campus Map | Asset Forge, Unity

- Built low-poly 3D building models and integrated them into a spatially accurate Unity scene to form the visual foundation of a campus digital twin.
- Implemented key systems for the digital-twin prototype, including first-person navigation, fast-travel nodes, and real-time facility/event overlays, to support interactive campus exploration.

## SKILLS

---

**Languages:** C, C++, C#, Python, Go, Bash, MATLAB, SQL

**Frameworks/Tools:** LangChain, PyTorch, ChromaDB, TensorFlow, YOLO, OpenCV, Pandas, Selenium, Unity, AssetForge, Canva, QGIS, FastAPI

**Certifications:** Deep Learning Fundamentals | Nvidia

## EXTRACURRICULAR ACTIVITIES

---

### **Orientation Management Committee Volunteer**

*LUMS*

Summer 2023

*Lahore, Pakistan*

- Ran onsite check-ins, campus walk-throughs, and small group briefings for ~ 1100 incoming first-year students during orientation week.
- Managed logistics for 12+ orientation activities and handled student operational queries throughout the on-boarding period.

### **Department Director - Media & IT**

*LUMS Students' Mathematics Society*

2022 – 2024

*Lahore, Pakstan*

- Managed society's digital presence across social media platforms and led a team of 8 members to coordinate media strategy and content creation.
- Designed promotional materials for academic events using Canva, creating posters, banners, and social media posts.

### **Event Head Math Gauge**

*SPADES @ LUMS*

Fall 2023

*Lahore, Pakistan*

- Designed and executed mathematical competitions and activities for ~ 40 high school teams over a 3 day flagship event.

### **Event Head Bingo**

*LUMS Students' Mathematics Society*

Fall 2022

*Lahore, Pakistan*

- Designed and executed a subcategory competition for ~ 100 high school participants.