AIZA ALI

Generative AI Engineer · LLM Applications · Multi-Agent Systems · RAG · Prompt Engineering

aiza.ali03@gmail.com | +92-300-8545676 | linkedin.com/in/aiza-ali-03-ai | github.com/blacksinisterx | Portfolio | Islamabad, Pakistan

Education

National University of Computer & Emerging Sciences (FAST-NUCES) — Islamabad, Pakistan
B.S. in Artificial Intelligence | CGPA: 3.62/4.0 — *Aug 2022 – Jun 2026*

- Dean's List: Semesters 1, 2, 4, 6, and 7 | Rector's List: Semester 8

Experience

AI Networks (Pvt) Ltd — Islamabad, Pakistan
Automation Engineer – AI Automation & Agentic AI Development — *Jul 2026 – Present*

- Built the real-time voice pipeline for **Jarvis/Sparkmind** on the **Gemini Live API**, with long-term memory and multiple LLM-backed agents for automated content generation.
- Shipped client websites (**MERN** stack) with SEO, deployed to production hosting.

FAST-NUCES — Islamabad, Pakistan
Teaching Assistant — *Aug 2025 – Jun 2026*

- **Agentic AI** (B.S., Spring 2026): Assisted in delivering course content on LLM-based autonomous agents, multi-agent systems, and tool-use frameworks; supported student evaluations.
- **Applied Programming** (M.S., Fall 2025): Graded assignments and mentored graduate students on computing fundamentals.

LMKR — Islamabad, Pakistan
AI Engineering Intern — *Jul 2024 – Aug 2024*

- Built a real-time facial recognition & geolocation security system using **OpenCV**, **dlib**, and **Flask**, achieving **90%** identification accuracy.

Research Projects

Seed-Free Data-to-Text Generation via LLM-Based Synthesis — 2025

- Designed a zero-shot LLM pipeline that cut annotation costs by up to **$50K** while matching fully supervised model performance on benchmark datasets.

Security Audit of Agentic AI Frameworks — LangChain · CrewAI · 2026

- Evaluated 5 adversarial attack types (prompt injection, memory poisoning, agent impersonation) across secured and vulnerable configurations, exposing critical multi-agent security gaps that persisted even under defenses.

FAST Federated Unlearning: Multi-Attack Evaluation — 2026

- Extended a published IEEE framework to remove backdoored knowledge from federated learning models, cutting attack success by ∼**90%** while preserving **99%** of clean-model accuracy.

Multi-Turn AI Safety Benchmarking Framework — 2025

- Built a local evaluation framework testing open-source LLMs (Llama3, Hermes3, Qwen2.5) against adversarial multi-turn conversations, introducing a new metric for context-accumulated risk.

Projects

DetectifAI – Intelligent Surveillance Platform *(Final Year Project)* — YOLO · CLIP · FaceNet · FastAPI · React

- Multimodal computer-vision and NLP platform for real-time CCTV threat detection, combining object detection, semantic video search, and facial identity tracking with a full storage backend.

Exploit-Path Tracer *(Live)* — Semgrep · LangGraph · Python AST · Next.js

- AI security agent that traces multi-hop vulnerability paths through uploaded codebases and auto-generates a proof-of-concept and fix, reasoning step-by-step to separate real risks from false positives.

Deposition Contradiction Finder *(Live)* — LangGraph · Supabase · Next.js

- AI legal-research agent that cross-references witness statements across multiple documents to flag genuine contradictions with exact citations.

AI Video Narrator – Local Browser TTS Pipeline — Kokoro TTS (ONNX/WASM) · ffmpeg.wasm

- Fully local script-to-narration pipeline: timestamp-aware sectioning, in-browser TTS synthesis, and burned-in captions with zero server calls or API keys.

Additional Projects — LangChain · CrewAI · F5-TTS

- **AI UX Auditor "Aura"** *(Live)* – hybrid audit agent (FastAPI, PaddleOCR, TensorFlow) with bounded LLM use; **Secure Multi-Tenant Agentic RAG System** (LangChain, CrewAI); **Story2Audio** – F5-TTS microservice converting storylines into emotionally expressive audio (gRPC, Gradio).
- **Agentic Airspace Copilot** (CrewAI, LangGraph, MCP); **LLM-Driven Disaster Response** (multi-agent ReAct/Reflexion/CoT simulation); **Agentic OCR** (VLM document extraction).
- **MPCount** & **Flight Delay Prediction** (deep-learning & ML pipelines); **Fact-Check Overlay**, **Clickbait Decoder** & **AI Slop Blocker** (Groq-powered Chrome extensions).

Technical Skills

Languages: Python, JavaScript/TypeScript, SQL, C++
GenAI & LLM: LangChain, LangGraph, CrewAI, RAG, MCP, ReAct/Reflexion/CoT, Prompt Engineering, LLM Fine-tuning, Vector Embeddings
Models & APIs: Gemini Live, Claude, Groq, Ollama, Hugging Face, F5-TTS, Kokoro TTS
Backend & Web: FastAPI, React, Next.js, Docker, Celery/Redis, PostgreSQL/Supabase, MongoDB
Tools: Git, Vercel, gRPC, Gradio, WebSockets