Karim

AI Systems Engineer
karim.ahmed4815@gmail.com

Experience

Senior Teaching Assistant - German University in Cairo

Sep 2025 - Present

Teaching Assistant - German University in Cairo

Sept 2024 - Sep 2025

Reference: Prof. Dr. Mervat Aboulkeir Email: mervat.abuelkheir@guc.edu.eg Reference: Dr. Ing Maggie Mashaly Email: maggie.ezzat@guc.edu.eg Facilitated hands on learning for ~250 students in CSEN 701 [Advanced Computer Lab] and Cloud Computing courses. The ACL Course is a practical lab that teaches 4th year Computer Science Students web development using the MERN stack, while the Cloud Computing course covers cloud concepts, services, and deployment models using VMware. I was responsible for adding a practical project to the Cloud Computing course curriculum where students replied to RFPs and presented their solutions based on what they learned throughout the course.

Software Engineer - Clynto

Jul 2024 - Oct 2024

Reference: Eng. Beshoy Louka Email: beshoy@clynto.com Developed and maintained the frontend application using Next.js, React, and Tailwind CSS while maintaining CI/CD pipelines. Contributed extensively to the GitHub frontend repository, consistently being one of the top contributors.

Education

Bachelor of Science in Computer Science and Engineering - German University in Cairo

2019 - 2024

Majored in Computer Science and Engineering with a Thesis in 3D Reconstruction of Human Characters

Master of Science in Computer Science and Engineering - German University in Cairo

2024 - 2025

Thesis Title: A Self Adaptive Agentic Moving Target Defense Architecture for Real Time Cyber Threat Response

Skills

- **AI/ML Frameworks:** TensorFlow, PyTorch, Scikit-learn
- **AI Applications & Development:** Reinforcement Learning, Agentic Systems, Adaptive Defense, RAG Pipelines, LLM Development
- **Full-Stack Development:** React, Next.js, Tailwind CSS, HTML5/CSS3, Node.js, Express.js, MERN Stack, RESTful APIs, MongoDB, SQL
- **Cloud & DevOps:** AWS, GCP, VMware, Docker, Kubernetes, CI/CD
- **Programming Languages:** Python, Java, JavaScript/TypeScript, Bash, C#
- **Research & Analysis:** Experimental Design, User Studies, Data Analysis, Technical Writing
- **Leadership & Soft Skills:** Teaching, Agile Methodology, Time Management, Communication, Teamwork

Projects

Multi-turn Multi-Agent System for Prompt Injection detection Portfolio

MAPD is a production-ready FastAPI service and research harness for detecting prompt injection/jailbreaks using a multi-agent LLM pipeline: Agents work to normalizes obfuscated prompts and judge them with optional ProtectedContext signals and an incremental history “unsure” loop for multi-turn cases. It supports Ollama or Gemini backends, detailed per-conversation logging and audit trails, a Vite frontend for interaction, and experiment tooling to run sweeps/ablations and generate metrics and figures for evaluation.

Personal Portfolio Portfolio

A high performance, design centric developer portfolio built to showcase advanced engineering capabilities. This project moves beyond static templates, implementing a full stack content management system (CMS) with production grade security and a premium design system.

Research Assistant - LLM Research Pipeline Portfolio

An intelligent, end to end pipeline for processing research PDFs using LLMs (Ollama or Gemini) with dynamic category generation, accurate PDF parsing with OCR fallback, LLM based metadata extraction, multi category scoring, deduplication, and topic focused summarization.

LLM-Powered Moving Target Defense for Real-Time Cyber Threat Response Portfolio

A self adaptive agentic architecture leveraging Large Language Models to orchestrate Moving Target Defense actions in real time, achieving automated incident response from detection to mitigation in under 2 minutes.

resbuilder Portfolio

This project was implemented as a reliability first resume transformation system that uses AI inside strict operational boundaries. The architecture combines meta prompting, evidence driven review, constrained building, rendering feedback loops, and multi layer validation to enforce factual grounding and one page A4 output. Production behavior is stabilized through queue based orchestration, stale job recovery, debug artifact observability, and CI/CD quality gates that block regressions before deployment.

rexlead Portfolio

Rexlead is a live lead intake and qualification system I built for my own services in AI systems, workflow automation, and software engineering. It combines...