Karim Ahmed

Cairo, Egypt • karim.ahmed4815@gmail.com • +201118808688 • LinkedIn • Substack • Portfolio

Cybersecurity Researcher & Engineer | (ISC)² Member | Specializing in AI-Driven Defense, Secure AI Systems, AI Integration and Cloud Security

Education

German University in Cairo (GUC) Cairo, Egypt
Master of Science in Computer Science and Engineering — Awarded July 2025
Thesis Title: A Self-Adaptive Agentic Moving Target Defense Architecture for Real-Time Cyber Threat Response

German University in Cairo (GUC) Cairo, Egypt
Bachelor of Science in Computer Science and Engineering — Awarded July 2024
Thesis Title: 3D Reconstruction of Human Characters

Experience

GUC - Teaching Assistant - Cairo, Egypt — Sep 2024 - Present
- Instructed more than 250 students Full-Stack development and Cloud Computing fundamentals.
- Introduced a new course, **Agentic AI development lab,** to be taught in the Spring 2026 semester.
- Co-founded the **Artificial Intelligence Research Lab GUC (AIRLab GUC),** which focuses on researching and developing new technologies for cybersecurity, cloud computing and NLP using Artificial Intelligence, launching Spring 2026.

Clynto - Remote - Software Engineer — Jul 2024 – Oct 2024
- Developed and maintained the frontend for the webApp, consistently being one of the top contributors.
- Initiated new security controls to further secure the online transactions using different threat models.

Certifications & Hands-On Training

ISC2 Certified in Cybersecurity (CC) - Credly
OWASP Top 10 - TryHackMe
AWS Cloud Practitioner CLF-C02 - Credly
Google Cybersecurity Professional Certificate - Coursera

Research and Projects

LLM-Powered Moving Target Defense — Master's Research — Self-adaptive agentic architecture leveraging LLMs to orchestrate moving target defense operations in real time, achieving sub-two-minute response cycles. - Portfolio Link
Free LLMs – Local AI Interface — Local interface for Ollama models offering offline access to open-source LLMs with multi-chat sessions, model management, and prompt customization. - GitHub
REX Scan – Penetration Testing Toolkit — Comprehensive reconnaissance and vulnerability-scanning framework integrating Nmap, Searchsploit, Gobuster, and SMB enumeration, with consolidated reporting. - GitHub
Stage Tracker – Pipeline Logging Tool — Python CLI utility and PyPI package for structured log collection and event tracking in CI/CD pipelines, improving visibility and debugging automation. - GitHub & PyPI
Research Assistant – Intelligent Literature Organizer — Python-based research workflow engine that automatically ingests, classifies, and tags academic papers using topic models and custom taxonomies, enabling structured corpora organization for rapid literature review. Published as a PyPI package with a clean CLI and modular architecture. - GitHub & PyPI

Skills & Interests

Technical: Python, Bash, Java, Javascript, Typescript, C; MySQL, NoSQL; git
Cloud & Infrastructure: AWS, Google Cloud Platform (GCP), VMware, Docker, Linux Systems, Windows Server
Security: Metasploit, MSFVenom, Caldera, CyberBattleSim, BurpSuite, Nmap, Wireshark, Suricata, Splunk and Snort
Frameworks & Standards: ISO 27001, MITRE ATT&CK & D3FEND, NIST CSF/RMF, STRIDE, PASTA, TRIKE
AI & Intelligent Systems: Agentic Design, LLM Orchestration, RAG, Local LLMs (Ollama), LangChain, HuggingFace, TensorFlow, PyTorch
Soft Skills: Agile Methodologies, problem-solving, effective communication, team collaboration, time management
Development & Automation: REST APIs, Microservices, CI/CD, PyPI Packaging, CLI Tooling, DevOps Practices