Syed Abdul Rasheed

AI Engineer: building, evaluating and securing AI agents

Islamabad, Pakistan (UTC+5), open to roles · pltr0116@gmail.com · syedrasheed.pages.dev · linkedin.com/in/syed-abdul-rasheed-8424382a4 · github.com/sar-04

SUMMARY

AI engineer who builds, evaluates and secures AI agents. A year of contract evaluation work for three AI labs, including leading a team of 5 that shipped over 200 agentic tasks. Built an agent security system deployed by a US client, and a multi camera computer vision system as my final year project.

EXPERIENCE

AI Evaluation Engineer (contract), three AI labs under NDA Nov 2025 to Oct 2026

- Lab 1 (Nov 2025 to Jul 2026): led a team of 5 task creators that shipped over 200 agentic tasks to the lab's specifications and difficulty targets, each with a reproducible Docker environment, task spec, human written reference solution and automated verifier suite for RL training and model evaluation.
- Automated the team's task QA with LLM judges that scored every task against a Terminal-Bench style rubric (prompt and grader alignment, task fairness, quality bar) before human review.
- Lab 2 (Apr 2026 to May 2026): Terminal-Bench style long horizon shell tasks. Lab 3 (Aug 2026 to Oct 2026): SWE-Bench style tasks on real repositories with failing tests.

AI Engineer, SWAM Technologies LLC (project based, hybrid) Jun 2025 to present

- Built an agent security system for a US client, deployed in their systems: prompt injection detection, cross tenant isolation, PII redaction, approval gated high risk actions, and a hardened MCP gateway and tool server with scoped, short lived tokens. Shipped with a red team evaluation harness and pytest security suite.
- Built an agentic invoice validator: LLM extraction from PDF invoices, field validation and cleaning, regenerated invoices and automated email delivery (Python, OpenAI API, OCR, Gradio).

Founder and Automation Engineer, visa appointment automation service Jul 2024 to May 2025

- Founded and ran a service that secured appointment bookings for more than 500 clients.
- Reverse engineered undocumented booking portal endpoints and session flows from network traffic; built resilient Python automation with session management, retries and monitoring.

PROJECTS

Agent security demo (public) github.com/sar-04/AI-SECURITY-PROJ

- Public version of my agent security design (input policy, injection firewall with an LLM judge, MCP gateway, tenant scoped retrieval). Built a labelled evaluation (44 attacks in 7 categories, 38 normal questions): 0 of 44 attacks leaked data. Documented that the keyword layer wrongly refused 7 of 8 technical questions, and fixed a fail open default and an ownership check bug.

Sentinel: multi camera vehicle re-identification (final year project) 2025 to 2026

- Multi stream RTSP ingestion and dashboard, natural language video search with Qwen3-VL embeddings, and a YOLOv8, ByteTrack and FastReID pipeline with Redis Streams (Python, PyTorch, FastAPI, React, Docker).
- Measured cross camera matching on all 409 tracks of CityFlowV2 scene S01 (716 true pairs among 66,087): travel time gating and one to one matching raised link precision from 17% to 83%.

EDUCATION

BS Artificial Intelligence, National University of Computer and Emerging Sciences (FAST-NUCES), Islamabad 2022 to Jul 2026

CGPA 3.1 / 4.0

SKILLS

Agents and evaluation	Agentic task authoring, Docker environments, verifiers, LLM as judge, SFT and RL datasets, LangChain, MCP
AI security	Prompt injection attack and defence, secure MCP design, agent hardening, red teaming
ML and vision	PyTorch, OpenCV, FastReID, YOLOv8, scikit-learn, pandas, NumPy
Backend and infra	Python, C++, SQL, Bash, FastAPI, Flask, Redis, MySQL, SQLite, Docker, Linux, Git, pytest, CI/CD
Automation and RE	Selenium, Playwright, Wireshark protocol analysis