Khubaib Alam

+92 335 2881372 khubaibalam2000@gmail.com linkedin.com/in/khubaib-alam github.com/khubaibalam2000
khubaibalam.com

Summary

AI & Agentic Software Engineer with 3 years shipping production systems across fintech, cross-border remittance, and security SaaS. Design and build **production AI agents on Anthropic Claude**: multi-agent pipelines that reason, plan, call tools, retrieve enterprise knowledge, and act under human approval, integrated with enterprise APIs, databases, logs, and mailboxes via **MCP** and custom tool interfaces. Strong in Python and Java/Spring Boot, structured LLM outputs, RAG-style retrieval, agent evaluation, and guardrails, with a security-first, human-in-the-loop mindset.

Experience

Techlogix **Sep 2023 – Present**
Senior Software Engineer *Karachi, Pakistan*

- **Agentic AI Support & SDLC Platform (Anthropic Claude)** | *Python, Claude (Opus/Sonnet/Haiku), MCP, FastAPI/Flask, SQLite, Oracle*
  - Designed and shipped a **production Claude agent** that turns a recurring enterprise support inbox into a review-and-send queue: a scheduled headless **Claude** run polls the mailbox, investigates each issue against the codebase, a read-only **Oracle** database and a curated knowledge base, and drafts an **evidence-cited** reply; **nothing sends without human approval**.
  - Generalized the same architecture and infrastructure into a **multi-project, AI-driven SDLC platform** to apply the workflow across the company: beyond triage and RCA, the agent proposes **code changes** end-to-end (branch → agent writes the change → build/tests → review → commit/push **bound to the exact diff**), making support and delivery an **AI-driven, human-approved** workflow.
  - Built the **tool-use / integration layer** over the **Model Context Protocol (MCP)** and custom connectors (mailbox via Microsoft Graph, Git repositories, SQL database, logs, SSH, ticketing) behind one **search/fetch tool contract**, read-only for evidence.
  - Architected the **multi-agent pipeline**: a planner (Claude Sonnet) selects lookups, the host retrieves evidence from every source, an investigator (Claude Opus) reasons and drafts, and a **verifier agent** checks each claim against cited evidence (plan → retrieve → reason → verify), all with **structured JSON outputs**.
  - Engineered **guardrails, evaluation and human-in-the-loop** controls: SELECT-only DB access, protected-branch git guard, an **ask-first gate** that raises a question over a low-confidence guess, plus automated verify/review gates, per-run confidence scoring and an audit trail.
  - Cut **token cost and latency** with **per-task model tiering** (Claude Opus for planning and reasoning, lighter Sonnet/Haiku models for mechanical work, plus reasoning-effort tuning) and tight **context engineering** (grep and line-range slices and log pre-filtering instead of whole files).
- **AlexBank (Egypt): Inward Remittance Platform** | *Java, Spring Boot, APIs, Oracle, Angular, Docker*
  - Contributed to a **cross-border inward remittance platform** enabling **GCC-to-Egypt** money transfers for retail customers.
  - Developed a **regulatory compliance microservice** to **block corporate transactions** and enforce person-to-person (P2P) remittances within a strict **two-month deadline**, preventing potential penalties from the **Central Bank of Egypt (CBE)**; integrated **Finacle Core Banking APIs** to validate customer type prior to processing.
  - Hardened application security with **HTTP-only**, **secure cookie-based authentication** and a single active session per user.
  - Configured centralized logging with **Graylog** to improve observability and cut incident resolution time; collaborated with the client's **Cairo team** and regional agents across **KSA, Oman, and UAE** for cross-border operations and rapid incident resolution.
- **Al-Fardan Exchange LLC (UAE): Fintech & Payments Platform** | *Java, Spring Boot, SQL Server, Angular, Azure*
  - Designed and implemented a **Bank Reconciliation module** (automated and manual) matching bank statements to Journal Vouchers, including a **regex-based auto-reconciliation** engine that cut manual effort.
  - Managed application deployments and automated **CI/CD pipelines on Azure** for high availability and streamlined delivery.
  - Enhanced the **Wages Protection System (WPS)** module with automated employer and employee notification workflows and payroll event handling.

VaultStrike **Oct 2023 – Present**
Co-Founder & Head of Engineering *Karachi, Pakistan*

Technologies: Python, Django, Next.js, PostgreSQL, GenAI, RAG, OpenAI

- Co-founded and engineered **Defbot**, a **multi-tenant SaaS web-security platform** (agentless cloud and agent-based deployments) with **granular Role-Based Access Control** and audit logging across CISO, compliance, and operations roles.
- Integrated a **GenAI security assistant** using **OpenAI APIs** with **RAG-based knowledge ingestion** to deliver contextual, product-aware guidance.
- Built **real-time website defacement detection** using continuous web scraping and user-defined regex/keyword monitoring.
- Developed centralized **vulnerability management** with **multi-channel alerting** (portal, email, Slack, webhooks) and **Twilio** voice calls for high-risk alerts.
- Built **External Attack Surface Management** (subdomain discovery, DNS health, exposed-email analysis) and unified alerting for uptime, TLS/domain expiry, malware, file integrity (FIM), and DNS/email security.
- Implemented **agent-based incident-response workflows**: website backup, defacement containment via maintenance-page deployment, and directory locking; collaborated with **DevOps** on CI/CD, containerization, and cloud infrastructure.

Freit.io **Jun 2022 – Aug 2022**
Software Development Intern *Karachi, Pakistan*

- Built features on an **MVC** Java Spring Boot + Angular application; tracked and enhanced APIs end-to-end with MySQL persistence.
- Wrote integration and automation tests with **Spring MockMvc** to ensure API functionality and reliability.

Education

National University of Computer & Emerging Sciences - CGPA: 3.45 **Aug. 2019 – Jun 2023**
Bachelor of Science in Software Engineering *Karachi, Pakistan*

Skills

- **AI / Agentic:** Anthropic Claude (Claude Code, Opus/Sonnet/Haiku), MCP (Model Context Protocol), tool use / function calling, structured outputs, multi-agent orchestration, RAG / knowledge retrieval, prompt & context engineering, agent evaluation, guardrails, OpenAI APIs
- **Languages:** Python, Java, TypeScript/JavaScript, C#, SQL, C/C++, HTML/CSS
- **Frameworks / Libraries:** Spring Boot, FastAPI, Django, Next.js, ReactJS, ASP.NET Core
- **Data / Cloud / DevOps:** Oracle, SQL Server, PostgreSQL, MySQL, Docker, Azure (CI/CD), Git/GitHub, Postman
- **Concepts:** Agentic workflows, multi-agent systems, human-in-the-loop, RAG, LLM evaluation, API security, JWT, microservices, multi-tenant design, system design, test automation, Agile/Scrum
- **Also:** Solved 400+ LeetCode problems (data structures & algorithms); designed scalable systems and modules from scratch; AI-assisted development with **Claude Code** and Cursor to accelerate delivery.

Achievements

- Dean's List: Awarded in 4^{th}, 7^{th} and 8^{th} semesters.
- System Design: **2^{nd} position** ACM DevDay Competition at FAST-NUCES; **CTF Runner-Up** (**3^{rd}**) in ACM Capture the Flag at FAST-NUCES.
- Best Internee: Recognized as **top performer** in the Data Science Department at SayabiDevs among 130 interns.
- **Open Source:** merged pull requests to **Microsoft** VS Code, **Google** web.dev, and **AWS** (dynamodb-encryption-python).

Certifications

- Spring Academy: Building a REST API with Spring Boot