

# TAIF AHMED TURJO

☎ +8801685840011 ✉ [ahmedtaif437@gmail.com](mailto:ahmedtaif437@gmail.com)  [LinkedIn](#)  [Github](#)

## EDUCATION

University of Dhaka

B.Sc in Computer Science & Engineering

2022 – Expected Graduation: February 2027

3.57 / 4 CGPA

## TECHNICAL SKILLS

**Languages:** Python, C/C++, Java, Rust, SQL, JavaScript, TypeScript, Bash, ARM Assembly, Dart

**ML Frameworks:** PyTorch, TensorFlow, scikit-learn, Hugging Face, CUDA

**Web & APIs:** FastAPI, Next.js, Node.js, React, RESTful APIs

**Data & Storage:** PostgreSQL (pgvector), Milvus, CockroachDB, Supabase, Firebase

**DevOps & Cloud:** AWS (EKS/ECS, ALB, CloudWatch), Docker, Railway, Kubernetes, CI/CD, Firecracker

**LLM & Agents:** Multi-agent orchestration, RAG, Model Context Protocol (MCP), prompt engineering, LangGraph, LangChain, CrewAI

## WORK EXPERIENCE

Rokkhe – Autonomous AI Penetration Testing Platform | [rokkhe.com](https://rokkhe.com)

June 2025 – Present

Founding Engineer

Remote

- Architected and built an autonomous AI penetration-testing engine that maps a target's attack surface and exploits it end-to-end without human steering, orchestrating multi-agent workflows over a 60-module extensible skill library spanning reconnaissance, cloud, protocol, framework, and vulnerability-class domains.
- Engineered the exploit-verification loop that separates the product from signature scanners: every finding is confirmed by generating and executing a working proof-of-concept inside a Docker-isolated sandbox, then auto-drafted into a remediation pull request via the GitHub API, converting raw findings into reviewed, merge-ready patches.
- Developed a full-stack control plane in FastAPI with WebSocket streaming for live agent telemetry, backed by TimescaleDB and Redis, enforcing multi-tenant workspace isolation at the query layer and pinning it with dedicated tenancy and authorization test modules.
- Built a provider-agnostic LLM abstraction over LiteLLM supporting OpenAI, Anthropic, and Google models under a bring-your-own-key model, alongside a sandboxed tool surface (headless browser automation, intercepting HTTP proxy, shell execution, patch application, web search) that agents compose at runtime.
- Shipped and operated the production deployment: a six-service Docker Compose stack behind Caddy with hardened security headers and content-hash asset fingerprinting, GitHub Actions CI across four parallel jobs publishing to GHCR, and zero-touch SSH rollout with graceful edge reload.
- Owned the public-facing surface end-to-end, implementing a schema.org JSON-LD entity graph, a per-bot crawler policy governing AI answer-engine access, IndexNow push indexing on every deploy, and Cloudflare edge protection with WAF rate limiting and Turnstile bot mitigation server-verified on all credential endpoints.

Makebell.com (Startup – Hong Kong)

October 2025 – May 2026

Software Engineer

Remote

- Architected and developed an end-to-end document intelligence and facts check pipeline for financial and legal documents (IPO prospectuses, fund factsheets), achieving a perfect extraction score on edge cases using a Docling-based preprocessor with custom table formatting fixes including merged cell forward-filling and row-span propagation.
- Engineered a multi-agent verification pipeline using Python FastAPI with parallel streaming architecture, reducing wall-clock processing time (latency cut by 70%) by eliminating redundant LLM calls through agent consolidation and concurrent execution.
- Developed DOCX MCP integration for live document editing and optimization, enabling real-time collaborative editing with AI-powered suggestions and automated formatting improvements with highlighting.
- Built a chunking orchestrator for structured document segmentation and developed stress-test corpora including synthetic edge-case documents to validate pipeline robustness across real Hong Kong IPO and KFS documents.

## Scale AI

December 2024 – January 2026

AI Trainer & L10 Reviewer

Remote - Contractual

- Fine-tuned and refined technical code in C, C++, Swift, Python, JavaScript, and Java to train and evaluate large language models, improving model reasoning, tool usage, and multi-step problem solving.
- Trained models and agents to recognize tools, reason about when and how to use them, and execute multi-agent workflows reliably.
- Designed adversarial prompts and stumper tasks to expose model failure points, edge-case vulnerabilities, and systematic reasoning errors.
- Built failure-driven training sequences to strengthen the model's handling of ambiguous, complex, and multi-layered reasoning and tool interaction.
- Contributed to OpenClaw's agent building across multiple AI models, aiming to reduce hallucinations and evaluating their outcomes.

## Turing

September 2025 – November 2025

Rust LLM Engineer - PR Writer V2 Project

Remote - Part Time

- Collaborated on **Anthropic's** PR Writer V2 initiative, evaluating and improving Claude's ability to generate production-ready Rust code.
- Conducted code reviews ensuring correctness, modularity, error handling, and performance, applying Rust best practices (cargo, dependency management, CI/CD).
- Developed build instructions, validated test suites, and identified issues in code quality, schema design, and recurring logic errors.
- Delivered structured QA reports and metrics on model performance to improve reliability in real-world Rust engineering workflows.

## SuperAnnotate

June 2024 – Present

Python AI Engineer & QA

Remote - Contractual

- Worked to generate an LLM's training data, Python, C, C++, HTML, Machine learning code snippets, its bugs and functions.
- Wrote prompt response on various programming and technical related(coding) questions (500+) required to train a chat-bot.

## PROJECTS

---

### AURORA – Auditable AI Research System | [Rust](#) | [GitHub](#)

2026

- Built an 8-crate Rust research system that turns questions into validated plans, retrieval tasks, evidence-backed claims, verification results, adaptive follow-up work, and grounded reports.
- Designed an auditable provenance chain using SHA-256-pinned source snapshots, exact excerpt validation, typed support/contradiction/sufficiency assessments, deterministic reconstruction, and claim-resolved citations.
- Added isolated adapters for OpenAI, Z.AI GLM-5.3, and Tavily with structured-output validation, cancellation, typed failures, and offline evaluation for unsupported claims, citation integrity, false completion, cost, and reproducibility.

### Hopper – VM Provisioning Platform | [Go](#), [FastAPI](#), [SvelteKit](#), [gRPC](#), [Kubernetes](#), [Longhorn](#) | [Github](#) | [Live](#)

2026

- Built core VM lifecycle on a Go/gRPC Kubernetes orchestrator with a FastAPI gateway and SvelteKit console: stop/resume/extend, persistent per-user workspaces (PVCs), DB-backed plan/image catalogues, and credit-based billing alerts over NATS JetStream.
- Led end-to-end adoption of Longhorn distributed block storage: replicated student workspaces with online volume expansion and admin resize, Azure Blob backup + DR runbooks, and measured node capacity fed through Protobuf into the admission scheduler – degrading gracefully to local-path when absent.
- Shipped the admin operations suite (per-user quotas, plan pricing, node/storage dashboards, audit-log export to CSV/JSON, issue resolution, force-terminate) with session TTLs and idle auto-shutdown, keeping a 590+ test suite (pytest, vitest, Go) green in CI.

### Cody – Collaborative Coding Platform | [Next.js](#), [FastAPI](#), [CockroachDB](#), [WebSocket](#), [Docker](#), [Monaco](#) | [Github](#)

2025

- Architected a real-time collaborative IDE, shipping user/project management, file system CRUD, invitations with RBAC, and WebSocket presence across projects.
- Designed the system for CRDT-based co-editing and sandboxed code execution (Docker), with clear security/perf targets ( $\leq 100\text{ms}$  event propagation,  $\leq 500\text{ms}$  API response).
- Implemented search, binary file handling, auto-save/tabbed editing, and a role-aware invitation flow (7-day expiry), aligning backlog and milestones toward production readiness.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>AFT-FTS (Advanced P2P File Transfer System)</b>   <i>Java, TypeScript, Spring Boot, React</i>   <a href="#">Github</a>                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>August 2025</b>   |
| <ul style="list-style-type: none"> <li>Designed and implemented a peer-to-peer file transfer system with adaptive networking, achieving 30% faster transfer speeds under fluctuating bandwidth.</li> <li>Integrated crash recovery and fault tolerance mechanisms, ensuring 99.9% uptime during stress tests.</li> <li>Secured communication with AES encryption, protecting 100% of file transfers against unauthorized access.</li> </ul>                                                                                                                         |                      |
| <b>Awaaz - Women's Safety App</b>   <i>Flutter, Firebase, Supabase</i>   <a href="#">Github</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>February 2024</b> |
| <ul style="list-style-type: none"> <li>Developed women's safety app enabling real-time SOS alerts with less than 3 second response time in emergency mode.</li> <li>Designed a Reddit like community section where verified users can post, vote, and comment, engaging to an impactful and reliable helping media.</li> <li>Implemented GPS-based tracking and safety zone analysis, covering 500+ unique locations during testing.</li> <li>Optimized UI/UX for dual interface navigation, improving usability scores by 25% in user feedback surveys.</li> </ul> |                      |
| <b>Uddhar – Tragedy Aid Management System</b>   <i>Next.js, React, PostgreSQL</i>   <a href="#">Github</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>March 2024</b>    |
| <ul style="list-style-type: none"> <li>Built a centralized platform to manage relief efforts, documenting aid distribution for 1,000+ victims across NGOs and government bodies.</li> <li>Streamlined support tracking (medical, financial, housing) using PostgreSQL, reducing data retrieval time by 40%.</li> <li>Deployed transparent history records, improving accountability and audit readiness by 30%.</li> </ul>                                                                                                                                          |                      |
| <b>Blood4Life – Blood Bank Application</b>   <i>Java, IntelliJ, JavaFX</i>   <a href="#">Github</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>May 2024</b>      |
| <ul style="list-style-type: none"> <li>Engineered a donor–recipient matching system with integrated maps, enabling 70% faster donor searches.</li> <li>Built real-time chatbox feature, connecting 50+ users during pilot phase with direct donor communication.</li> <li>Automated blood donation campaign updates, boosting community participation by 20%.</li> </ul>                                                                                                                                                                                            |                      |
| <b>PawTopia</b>   <i>Flutter, PostgreSQL</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>October 2023</b>  |
| <ul style="list-style-type: none"> <li>Developed a pet adoption and lost pet tracking app, registering 200+ adoption listings in initial rollout.</li> <li>Integrated e-commerce module for pet products, enabling secure transactions with 95% checkout success rate.</li> <li>Built community engagement features (posts, forums), increasing user retention by 15%.</li> </ul>                                                                                                                                                                                   |                      |
| <b>Minesweeper with Treasure Hunt</b>   <i>C++, Qt Framework</i>   <a href="#">Github</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>November 2023</b> |
| <ul style="list-style-type: none"> <li>Recreated Minesweeper with custom story mode and progressive difficulty. Implemented timer, flagging, and randomized grid generation for dynamic gameplay.</li> <li>Optimized rendering with Qt Framework, reducing game load time.</li> </ul>                                                                                                                                                                                                                                                                               |                      |

## HONORS & ACHIEVEMENTS

|                                                                 |                  |
|-----------------------------------------------------------------|------------------|
| <b>Champion</b>                                                 | <b>June 2026</b> |
| NSUCEC Cybernauts CTF held at NSU Campus                        |                  |
| <i>Inter-University Cybersecurity Event (Capture-The-Flag).</i> |                  |
| <b>12th Place</b>                                               | <b>May 2025</b>  |
| University of Asia Pacific CyberSiege                           |                  |
| <i>Inter-University Cybersecurity Event (Capture-The-Flag).</i> |                  |