

Swagato Bauri

[Linkedin](#) • [Github](#) • [HackerRank](#) • [Codeforces](#) • [Leetcode](#)



PROFESSIONAL SUMMARY

Full-Stack Developer & Agentic AI builder. 500+ DSA problems solved, LeetCode Rating: 1700+ (Top 12%), Codeforces 1050+. Skilled in C++, Python, and JavaScript.

EDUCATION

Bachelor of Technology (Artificial intelligence)	2024 - 2028
Newton School of Technology, Rishihood University	Grade: Pursuing
Intermediate (Class XII)	2023 - 2024
Jawahar Navodaya Vidyalaya	Grade: 7.5/10.0
Matriculation (Class X)	2020 - 2021
Jawahar Navodaya Vidyalaya	Grade: 92.0%

EXPERIENCE

Artificial Intelligence Engineer August 2026 - Present
Patchifi *Dubai, United Arab Emirates (Remote)*

- **Engineered an autonomous, multi-tenant security remediation engine** using AWS Bedrock (Anthropic Claude), automating vulnerability triage and patch scheduling across distributed endpoints.
- **Architected an event-driven serverless pipeline** leveraging AWS Lambda and Amazon EventBridge to execute scheduled, isolated AI agent sessions with strict tenant-level data segregation.
- **Designed and implemented contextual Action Groups via OpenAPI schemas**, enabling the LLM to securely fetch asset inventories, maintenance windows, and historical failure data for risk-prioritized decision making.
- **Automated cloud-native infrastructure provisioning** using Terraform (IaC), streamlining the deployment of Bedrock Agents, Lambda handlers, IAM roles, and AWS Secrets Manager with zero-downtime CI/CD practices.
- **Streamlined the vulnerability patching lifecycle**, bridging the gap between security alerts and execution by generating automated, compliance-aware Draft Remediation Plans without human intervention.

Open Source Contributor June 2026 - Present
krkn-chaos (CNCF Sandbox Project, Red Hat) *Remote*

- **Shipped 7 merged pull requests** across krkn, krkn-hub, and the krkn-chaos website — a CNCF chaos engineering toolkit for Kubernetes/OpenShift resilience testing.
- **Designed and implemented an event-driven HTTP Trigger framework** for krkn (#1504), letting chaos scenarios fire on external webhook events instead of static schedules; extended the integration in krkn-hub (#358) and authored the user-facing documentation (website #572).
- **Built the node-network-chaos scenario end-to-end** — implemented the krknctl scenario image (krkn-hub #354) and wrote the accompanying documentation (website #555) — giving users a CLI-driven way to inject network faults on target nodes.
- **Added parallel pod deletion support** to the Pod Disruption scenario (krkn #1536), enabling simulated simultaneous quorum loss instead of default serial rollout, with matching docs (website #587).
- Collaborated directly with maintainer **Darshan Jain (@ddjain)** across review cycles on all merged contributions.

INTERNSHIPS

Full Stack AI Developer June 2026 - Present
CareerCafe *Remote*

- Built a rule engine that evaluates student interview responses against structured criteria, serving 100+ daily active users on a live AI interview platform.
- Engineered dynamic follow-up route logic that generates contextual interview questions based on prior response analysis.
- Shipped backend features end-to-end across route design, business logic, and database integration on a production system.

PROJECTS

TARS - Threat Analysis & Response System ([Github](#)) ([Demo](#)) March 2026

- Built an autonomous cybersecurity agent that closes the **detect → alert → wait-for-human** gap by reasoning about threats and executing defensive actions within milliseconds, without human intervention.
- Architected a **7-stage closed-loop defense pipeline** (Observe → Analyze → Reason → Decide → Act → Learn → Validate) over **FastAPI + Celery + Redis pub/sub**, where ML inference and response execution never block the log ingestion path.
- Engineered a **confidence-gated execution engine** with Shadow, Human-Approval, and Autonomous modes — scoring false positive risk across **5 behavioral factors** before any action fires, with a **7-day shadow observation period** before enabling live responses.
- Built a **deterministic ScoringEngine** combining **Isolation Forest + One-Class SVM** (0.6/0.4 weighted) with kill chain multipliers and **EMA-adjusted thresholds** — Groq LLM restricted to explainability only, keeping every decision fully auditable.
- Implemented a **4-stage Kill Chain Tracker** (Recon → Enumeration → Exploitation → Persistence) that proactively escalates responses as attackers advance, and an **Adversarial War Games engine** where the simulated attacker adapts strategy when blocked — achieving **87–100% detection rates** across all attack vectors.

ULTRON ([Github](#)) ([Demo](#)) January 2026

- Built a **6-node directed acyclic graph (DAG)** using LangGraph's **StateGraph** with **conditional edge routing**, where each node is an AI agent and the execution path adapts at runtime based on what the previous agent returned.
- Implemented a **non-blocking streaming architecture** using Python's thread-safe **Queue**, Flask's **StreamWithContext**, and **Server-Sent Events (SSE)** to push live per-agent updates to the frontend with zero main-thread blocking.
- Engineered a **self-healing revision loop** between Critic and Content Creator nodes using **TypedDict shared state**, **Annotated list fields**, and **operator.add reducers** — with a **circuit breaker pattern** via revision count guards to prevent infinite cycles.

- Integrated **Google Search API** into the Researcher Agent's **inference pipeline**, injecting live web results into LLM prompts to ground outputs in real-time trends rather than relying solely on training data.

SKILLS

Computer Language: C++, JavaScript, Python, SQL, TypeScript

Databases & Data Tools: MongoDB, MySQL

AI / ML: GenAI, LangChain, LangGraph, Machine Learning

Cloud & DevOps: Docker

Frameworks & Libraries: Express JS, Node.js, Prisma ORM, React, Tailwind

EXTRA-CURRICULAR ACTIVITIES

- **Award-winning photographer** with national and international recognition
- **Flautist**, trained in Indian classical music