Rahul Paul

+91 9163130524 | rahulpaul.csetech@gmail.com | LinkedIn ↗ | GitHub ↗ | LeetCode ↗ | Portfolio ↗

Education

MS Ramaiah Institute of Technology — Bengaluru, Karnataka
B.E. in Computer Science and Engineering (Cyber Security) — *2023 - 2027*
- CGPA: **9.52 / 10.0**

Bhavan's Gangabux Kanoria Vidyamandir — Kolkata, West Bengal
*Class XII (AISSCE) — **96.33%*** — *2021 - 2022*

Work Experience

Project Intern - Samsung Prism | **Samsung R&D Institute India** | Bengaluru — *Dec 2025 – Present*
- Developing **EmoCapNet**, a **254.8M-param** multimodal vision-language model for **7-class emotion-aware image captioning**, fusing **ViT-Base + GPT-2** via cross-attention and **VAD-FiLM** conditioning with multi-task learning (captioning, VAD regression, emotion classification, contrastive alignment) on a 67K-caption emotion-augmented **Flickr30k** corpus.
- Distilled the teacher into a **TinyCLIP-ViT + DistilGPT-2** student (**112.5M params, 2.3× smaller**) — **METEOR 22.1**, **CIDEr 0.363**, emotion-controllability **r = 0.81** — then shipped on-device via **INT8 dynamic quantization**, compressing **∼1GB → 153MB** (**6.7×**) with from-scratch **KV-cache** decoding and an **ONNX/TorchScript** export path.

Projects

Sentinel – Autonomous AppSec Agent | GitHub ↗ — *Jun 2026 – Jul 2026*
- Built an **autonomous AppSec agent** that **finds, proves, and fixes** source-code vulnerabilities: an **LLM** surfaces candidate flaws, then a **validator proves each with a generated proof-of-concept exploit** executed in a locked-down, **network-disabled Docker sandbox** – unproven findings are discarded, **driving false positives toward zero**.
- Made the model layer **provider-agnostic** via **LiteLLM** (Ollama / Claude / OpenAI) and added a **secure-fix patcher** behind a **human-approval gate**; a **self-correction loop** raised **recall 60% → 100%** (precision 100%) across **five vulnerability classes** on a reproducible eval harness, inspired by **DARPA's AI Cyber Challenge**.

Tech: Python, LiteLLM, Ollama/Claude/OpenAI, Docker, Python AST, difflib, pytest, GitHub Actions

Smart Course Generator | GitHub ↗ | Live Demo ↗ — *May 2026 – Jun 2026*
- Built a full-stack **AI learning platform** that generates structured multi-module courses and **streams them lesson-by-lesson over SSE**, with adaptive quizzes, flashcards, and an **AI-scored mock-interview** mode; secured with rotating **reuse-detecting refresh-token auth**, **Zod** validation, and rate limiting.
- Engineered a custom **multi-provider AI router** (**Gemini → Groq → OpenRouter**) with per-provider **circuit breakers**, retries, timeouts, and API-key rotation, and made generation quality **measurable** via an **LLM-as-judge eval harness** with **RAG** grounding, wired into **CI**.

Tech: React, TypeScript, Node.js, Express, MongoDB, Gemini/Groq/OpenRouter, SSE, Zod, Jest, Playwright, GitHub Actions

Rubik's Cube Studio | GitHub ↗ | Live Demo ↗ — *Mar 2026 – Apr 2026*
- Implemented **Kociemba's two-phase algorithm** from scratch in **TypeScript** (cubie model, phase-wise **coordinate reduction**, precomputed **pruning tables**, **IDA* search**) — averaging **∼20.6 moves** (God's number is 20) at **100% correctness across 1,500+ random cubes** vs. an independent reference engine.
- Ran the solver in a **Web Worker** to drive a stutter-free **Three.js** 3D animation, added **webcam cube scanning** via an HSV color pipeline, and shipped with **66 unit tests**, Playwright E2E, and strict TypeScript.

Tech: TypeScript, Three.js, Web Workers, Vite, Vitest, Playwright, GitHub Actions

DNSentinel – DNS Threat Intelligence Platform | GitHub ↗ | Live Demo ↗ — *Apr 2026 – Jun 2026*
- Built a full-stack **DNS threat-detection platform** detecting **DGA**, **tunneling**, **exfiltration**, and **C2 beaconing** via a **22-feature RF + Isolation Forest ensemble**, driving a **SOAR** auto-block/sinkhole layer mapped to **MITRE ATT&CK**; validated across **25 real DGA families** with **SHAP**-explained reports.

Tech: Python, FastAPI, React, scikit-learn, Docker, Chrome MV3, pytest, GitHub Actions

Publications

Applications of Quantum Computing for Internet of Things | **Springer Nature** | Publication ↗ — *2025*
- Co-authored a **43-page Springer Nature book chapter** (pp. 79–121) in *Quantum Computing, Sensing and Communications for IoT*, **surveying 70+ papers** on the integration of **Quantum Computing with IoT** for security, optimization, and intelligent decision-making across **Quantum ML**, **Post-Quantum Cryptography**, and **Quantum Sensing**.

Technical Skills

- **Languages:** Python, C/C++, TypeScript, JavaScript, SQL
- **AI/ML:** PyTorch, Transformers (ViT, GPT-2), Vision-Language Models, Knowledge Distillation, INT8 Quantization, ONNX, scikit-learn
- **GenAI & Web:** LLM Integration, RAG, Prompt Engineering, Multi-provider AI Routing, React, Node.js, Express, FastAPI, SSE, JWT/OAuth2
- **Data & DevOps:** MongoDB, Docker, Git, GitHub Actions (CI/CD), Jest, Vitest, Playwright, pytest; DSA, OOP, DBMS, Computer Networks, Cyber Security

Achievements & Certifications

- **LeetCode:** Contest Rating **1821 — top 7.32% globally** (17 rated contests) | Profile ↗
- **Campus Ambassador — Kshitij, IIT Kharagpur** | Certificate ↗
- **Certifications:** IBM — Threat Intelligence & Hunting, IBM — Security Operations in Practice, Infosys Springboard — DSA