Satyam Pratik Bharti

Bengaluru, India — Open to Relocation / Remote / Onsite
bharti.satyamspb@gmail.com — +91 6204764664 — GitHub — LinkedIn — LeetCode — X — Portfolio

SUMMARY

Full-stack software engineer specializing in building scalable web applications and AI-powered systems using React, FastAPI, TypeScript, and MongoDB. Hands-on experience with LLM fine-tuning, RAG pipelines, embeddings, adversarial NLP evaluation, and production deployment of AI-driven features. Strong foundation in Java, OOP, and DSA with a focus on clean architecture and production-quality engineering.

SKILLS

Languages: Java, TypeScript, JavaScript, Python
Frameworks / Tools: React, Node.js, Express.js, FastAPI, Tailwind, LangChain, scikit-learn, Git, Postman
Databases: MongoDB, MySQL
ML / AI: RAG, LoRA, Embeddings, SMOTE, TextAttack (TextFooler, DeepWordBug, BAE)
Concepts: LLM Security, Adversarial NLP, REST APIs, JWT Auth

EXPERIENCE

AI Safety Research Collaborator — Samsung PRISM *11/2023 – 10/2024*

- Researched adversarial prompt-injection vulnerabilities in transformer-based LLMs using TextAttack across models including DistilBERT and Llama-3.1.
- Fine-tuned **Llama-3.1-8B** using LoRA and 4-bit quantization via Unsloth, completing training in **7.12 minutes** with **52.7% peak GPU memory utilization**, improving refusal consistency under adversarial evaluation.
- Published an adversarial dataset of **61,857 samples** combining Alpaca-cleaned and custom hostile-instruction prompts to enable reproducible robustness research.
- Completed the full PRISM project scope under SRI-B mentorship, delivering all planned milestones to conclusion.

PROJECTS

CosmiLearn — Full-Stack AI-Powered E-Learning Platform GitHub
Production Deployment

- Built an adaptive learning platform supporting real-time AI tutoring and quizzes using React + Vite, TypeScript, Tailwind, FastAPI, MongoDB, and Groq Llama-3.1.
- Implemented a **RAG-based recommendation engine** using MiniLM embeddings and cosine similarity to generate personalized course suggestions.
- Deployed frontend via Vercel and backend on Hugging Face Spaces, integrating JWT auth, rate-limiting (SlowAPI), AbuseIPDB filtering, and streaming inference.

SMOTE-Enhanced Intrusion Detection System GitHub

- Developed a multi-class intrusion detection system detecting attacks including Blackhole, Flooding, and Selective Forwarding with **up to 97% accuracy**.
- Applied **SMOTE** to balance dataset distribution, improving minority-class recall by **over 35%**.
- Benchmarked ML models including SVM, RF, XGBoost, KNN, and Decision Trees using confusion matrices and ROC analysis.

EDUCATION

Bachelor of Engineering — Computer Science and Engineering
Visvesvaraya Technological University, Bengaluru, Karnataka
CGPA: 8.5 / 10 *05/2022 – 04/2026*