Aditya Shibu

New Delhi, India adityashibu275898@gmail.com 7683049759 in/adityashibu41148 github.com/Vic-41148

SUMMARY

BCA AI & DS student with shipped production projects — a live LLM security platform, a national hackathon AI system, and a real-world IoT solution. I build things that work.

EXPERIENCE

Full-Stack AI Security Engineer February 2026 – Present, New Delhi, India
KR Mangalam University

- Built a full-stack LLM security platform (Neuro-Sentry) deployed on Vercel + Railway, simulating and detecting 15+ prompt injection and jailbreak attack vectors across multiple AI models in real time.
- Engineered a 3-stage hybrid defense pipeline (rule engine → LLM classifier → score fusion) with a fast-block path for high-confidence attacks, cutting successful jailbreaks by 78%.
- Architected FastAPI backend with adaptive session-level threat tracking, handling 100+ concurrent evaluation requests at sub-200ms response time across 8 threat categories.
- Led a 4-person red/blue team evaluating 200+ AI vulnerability scenarios, coordinating attack simulation and defense tuning to improve overall detection accuracy by 35%.

Full-Stack AI Engineer March 2026 – March 2026, Surat, India
National Hackathon 2026

- Built SmartDesk, an AI-powered complaint management system using MERN stack, integrating Groq (llama-3.3-70b) and Gemini 1.5 Flash for intelligent ticket routing and automated L1 query deflection.
- Designed real-time agent dashboard using React and Socket.IO, streaming live ticket updates to multiple concurrent agents with JWT-secured authentication, bcrypt password hashing, and role-based access control.
- Implemented NLP-based emotion and severity detection classifying user sentiment across 5 categories and 4 priority levels, enabling automated triage without manual agent intervention.
- Delivered end-to-end system handling 50+ concurrent users with MongoDB Atlas backend, CSV export, analytics charts, multilingual chatbot support, and satisfaction rating feedback within hackathon timeframe.

Robotics Engineering Intern June 2025 – July 2025, India, Delhi
Rotors

- Designed a smart IoT-enabled livestock collar monitoring health metrics (temperature, heart rate) and GPS location for 100+ animals simultaneously with continuous data logging.
- Integrated 5+ sensor modules, 2 microcontrollers, and Bluetooth communication systems achieving real-time data transmission with under 2-second latency across field conditions.
- Collaborated with a 4-member multidisciplinary team to prototype, field-test, and present the fully functional device to company leadership, completing all deliverables within the internship timeframe.

Systems Security Engineer February 2026 – February 2026, New Delhi, India
KR Mangalam University — IBM ThinkFest 2026

- Built CodeShield, a multi-threaded log anomaly detection engine in C using pthread-based concurrency, processing 1200+ log entries with real-time threat scoring and automated alert generation.
- Developed scoring and alert systems (scorer.c, window.c, alert.c) implementing a custom anomaly formula (failed×3 + resources×2 + ips×4) with color-coded severity classification and circular alert queue.
- Engineered a sliding 5-minute time-window with O(1) reference-counted stat updates, enabling real-time pattern detection across concurrent log streams with modular pipeline designed for SIEM extensibility.

EDUCATION

Bachelor of Computer Applications (BCA)
Minor in Robotics K.R. Mangalam University Sohna, Haryana 2026

SKILLS

Languages: Python, C++, C, Java, JavaScript, TypeScript, Kotlin, SQL
Frameworks & Tools: React, FastAPI, Node.js, Express.js, Flask, Socket.IO, MongoDB, Vite, Docker, Vercel, Railway, Git, Arduino IDE, PlatformIO, Postman
Domains: AI/ML, LLM Security & Red Teaming, Full-Stack Web Development, Systems Programming, Embedded Systems & IoT, Real-Time Systems