

Adarsh Arun

Bengaluru, India | +91 8085446706 | adarsh3arun@gmail.com | [linkedin.com/in/adarsh3arun](https://www.linkedin.com/in/adarsh3arun) | github.com/Adarsh04Arun

Education

B.N.M Institute of Technology, BE in Computer Science and Engineering – Bengaluru, KA Aug 2023 – present

- CGPA: 9.70

Experience

AI Safeguards Engineering Intern, XelerAIT – Remote, Bengaluru, KA Aug 2026 – present

- Contributing to the development of a comprehensive guardrails framework for AI-driven healthcare solutions.
- Designing and implementing guardrails for production-grade agentic AI frameworks to ensure safety, reliability, and compliance in healthcare applications.

Software Development Intern, Nife Labs – Remote, Singapore Nov 2025 – May 2026

- Developed an enterprise-grade AI management solution designed to facilitate secure and compliant interactions with external Large Language Models.
- Implemented a configurable compliance architecture enabling organizations to enforce proprietary security standards and operational guardrails.
- Engineered token optimization strategies to reduce inference cost and latency.

Projects

Prompt Enhancement Engine (ISTVON Framework) – Python, Streamlit, Gemini API

- Built a Streamlit AI security engine with Python and the Gemini API to analyze, enhance, and secure LLM prompts.
- Engineered a dual-layer security broker utilizing regex and metaprompts to block injection attacks and semantic threats.
- Architected the ISTVON JSON framework to structure and sanitize unstructured text, isolating malicious payloads.
- Integrated a comprehensive audit trail and unit-testing suite to log verdicts and ensure high-fidelity threat detection.

Telecom Security Operations Center (SOC) Simulation – Python, RAG, LLMs, AutoAI

- Engineered a Python DFIR pipeline automating ETL processes and threat detection via MDE Investigation Packages.
- Leveraged AutoAI for predictive threat scoring and LLMs for automated, structured incident reporting.
- Implemented a RAG architecture to intelligently map simulated attack patterns directly to the MITRE ATT&CK framework.
- Automated log parsing and visualization to streamline intrusion analysis and minimize manual investigation overhead.

Adaptive Triage Engine for SOC – Python, Contextual Bandits, Scikit-learn

- Developed a Python incident triage agent to optimize response workflows and accelerate threat escalations.
- Implemented a Contextual Bandit (RL) algorithm to score and triage alerts dynamically using forensic feature data.
- Built data pipelines to ingest, normalize, and parse raw security logs into structured real-time threat telemetry.
- Evaluated policy stability using analytics tracking reward distributions, confusion matrices, and precision-recall trade-offs.

Multi-Client Group Chat Application – Java, TCP/IP Sockets, Swing/AWT

- Engineered a real-time messaging platform using Java Socket Programming (TCP/IP) for low-latency communication.
- Implemented multi-threaded server logic to handle concurrent client connections and synchronized broadcasting.
- Designed an asynchronous GUI using Java Swing and AWT to enable dynamic, lag-free user chat sessions.

Achievements

3rd Place – HackFusion 1.0, Maharaja Institute of Technology – Mysore Sept 2025

- Awarded for developing an AI-based solution showcasing practical innovation and teamwork in a 24-hour national-level hackathon.
- Recognized for strong technical execution and problem-solving under time constraints.

Professional Development

PwC Launchpad – SAP S/4HANA Track, PwC India 2026

- Completed industry-focused training in SAP S/4HANA, Java, SQL, MongoDB, and Generative AI.
- Gained hands-on exposure to ERP workflows, database systems, and enterprise application development.
- Successfully completed program assessments and learning milestones.

Skills

Programming Languages: JavaScript, TypeScript, Python, Java, C/C++, HTML/CSS, SQL

Core Frameworks & Web: Next.js, React, Tailwind CSS, Node.js, Express, Streamlit

AI, Data Science & Security: LangChain, LlamaIndex, Google Agent Development Kit (ADK), Gemini API, Claude API, TensorFlow, Scikit-learn, AutoAI, Pandas, NumPy, Matplotlib, Plotly, OpenCV

Developer Tools & Databases: MongoDB, Git, Docker, UNIX/WSL, AWS, Google Cloud Platform (GCP), IBM Tools, Node-RED, Arduino IDE