

Santhana Bharathi M

Chennai, India

+91 6374131726 | santhanabharathim2001@gmail.com

linkedin.com/in/santhanabharathi | github.com/SanthanaBharathiM | Portfolio Website

Professional Summary

AI/ML Engineer with 2+ years of production experience architecting **Autonomous Agents** and **High-Throughput Data Pipelines**. Specialized in **Generative AI Ops**, building "Text-to-Action" tools using **MCP**, and deploying scalable **RAG systems** on AWS. Expertise in fine-tuning LLMs and engineering self-healing streaming architectures (Kafka/Flink) that process millions of events with sub-second latency.

Core Skills

Agentic AI & GenAI: LangChain, LangGraph, Model Context Protocol (MCP), RAG, GuardrailsAI, QLoRA Fine-tuning, OpenAI API, Llama-2, Mistral
Data Engineering: Apache Kafka, PySpark Structured Streaming, Elasticsearch, Apache Flink, Airflow, SQL
MLOps & Cloud: AWS (EC2, S3, EKS, CloudWatch), Docker, Kubernetes, CI/CD Pipelines, FastAPI Serving
Programming: Python (Expert), SQL, JavaScript, Java, Shell Scripting
Security Domains: UEBA, MITRE ATT&CK, Threat Intelligence, Network Anomaly Detection

Professional Experience

Junior Developer (AI/ML & Security Ops)

Yakshna Technologies

06/2025 – Present

Chennai, India

- Architected a real-time Threat Detection Engine processing **2M+ events/day**. Integrated **Apache Kafka** for ingestion and **PySpark** for feature engineering, reducing detection latency from minutes to **<200ms**.
- Engineered a **Dynamic Risk Scoring Model (UEBA)** using Isolation Forests; drastically reduced false positives by **60%** by analyzing behavioral context rather than static rules.
- Implemented **Multi-Agent Orchestration (MCP)** to automate incident response; built agents that autonomously query Elasticsearch logs and propose remediation steps, cutting analyst triage time in half.
- Deployed **Self-Healing Airflow Pipelines** for batch model retraining; designed automated rollback mechanisms on AWS to ensure 99.9% system availability.

AI/ML Technical Consultant (Contract)

Yakshna Technologies

06/2024 – 06/2025

Chennai, India

- Designed a **"Natural Language-to-Selenium" Agent** using the **Model Context Protocol (MCP)**. Built a semantic router that translates plain English into executable browser actions, democratizing test automation.
- Reduced regression testing cycles by **45%** by implementing **Self-Correcting Selectors**; utilized LLMs to dynamically heal broken XPath locators during runtime execution.
- Optimized LLM inference costs for the internal automation tool by implementing vector caching layers and prompt compression techniques.

AI/ML Trainee

Yakshna Technologies

12/2023 – 06/2024

Chennai, India

- Fine-tuned Open Source LLMs (**Llama-2-7B, Mistral**) using **QLoRA** on custom cybersecurity datasets; improved MITRE ATT&CK classification accuracy by 18% over base models.
- Built a production-grade **RAG (Retrieval-Augmented Generation)** pipeline using LangChain; implemented Hybrid Search (Keyword + Semantic) to solve hallucination issues in customer support bots.
- Developed custom **Input/Output Guardrails** to prevent PII leakage and prompt injection attacks in client-facing AI applications.

Key Projects

GuardrailsAI + Local LLM Safety Framework | Open Source, Python, gpt-oss

- Developed a local safety layer for LLMs using GuardrailsAI; achieved **92% accuracy** in redacting sensitive PII and blocking jailbreak attempts in real-time.
- Built custom validators and architecture diagrams on GitHub, helping the community deploy secure, offline LLMs.

End-to-End UEBA Detection Pipeline | PySpark, Kafka, AWS, Docker

- Designed a scalable anomaly detection system: Kafka Ingestion → Spark Streaming → ML Inference → Kibana Dashboard.
- Handled high-velocity authentication logs (100K events/sec peak) with optimized partition strategies.

Publications & Community

- **Technical Writing:** Authored "How to Run LLaMA Models Locally" and "Cyber Threat Detection with ML" (Medium/Dev.to), garnering **8,000+ views**.
- **Continuous Learning:** Consistently updating skills via **Deep Learning A-Z™** (2025) and **Machine Learning A-Z™** (2024).

Education

B.Tech in Information Technology
IFET College of Engineering (Anna University)

06/2019 – 08/2023
GPA: 7.75 / 10