Nityashree S

AI Engineer · LLM agents, MCP, evals and AI security

+91 78270 76283 · nityashreesundararajan@gmail.com · India · **Portfolio** · LinkedIn · GitHub

SUMMARY

AI Engineer who builds and ships production LLM agents end to end at a payments startup: MCP connectors with per-user OAuth, evals, guardrails and AI red-teaming, built close to the teams who use them. I build by directing AI coding agents, and I own the design, the tests and every change that ships.

EXPERIENCE

AI Engineer · Yuno

Jun 2026 – Present

- Kept company-wide LLM agents reliable: root-caused a production outage to one malformed instruction file, and added timeouts, metrics and logs to the MCP tool gateway, which exposed a silently failing connector.
- Built a per-user OAuth 2.0 MCP connector so each employee's agent reaches only what that employee can see; designed and built multi-tenant guest access with isolated sessions and credentials.
- Red-teamed the agent engine before launch (prompt injection to guardrail removal and memory poisoning); the fix moved guardrails into the platform. Closed CSRF, webhook and fail-open auth gaps.
- Ran evals in production: shadow-tested a multilingual reply-language step on a labelled set before release, and an A/B test that led the team to change the default model.
- Fixed agent-session failures (duplicate or orphaned tool-call history that LLM providers rejected, failed turns that lost the user's message) and added a per-turn outcome record so agent success is measured in production.
- Built finance agents with the finance team (invoice intake: the LLM extracts, tested code validates) and a demo agent for a customer event.

Letter of recommendation from Yuno's VP of AI available on request.

Payments Analyst Intern · Yuno, Office of the CEO

Dec 2025 – Jun 2026

- Tested an internal AI assistant with Sales and BD before launch and caught the data error behind its wrong answers.
- Built a live KPI dashboard from Salesforce, MongoDB and Google Sheets APIs, and automated partner and payment-provider data upkeep.
- Built and audited a database of which payment providers and methods work in which markets, fixing data-quality errors.

PROJECTS

- **Smart Router** · LLM gateway that routes each prompt to a cheaper or stronger model, with fallback, Redis caching and cost logs · Live · Code
- **Meridian** · Multi-agent RAG research API: planner, parallel researchers, embedding ranking, critic and writer, streamed live · Live · Code
- **Cross-Border Fee API** · Itemises the cost of a cross-border payment: FX spread, fees and taxes · Live · Code
- **Fraud Pattern Explorer** · Risk-analyst dashboard with risk scores and suspicious-pattern alerts · Live · Code

SKILLS

AI: LLM agents, tool calling, MCP, RAG, prompt engineering, evals, guardrails, AI red-teaming

Engineering: Python, FastAPI, REST APIs, OAuth 2.0, SQL, Docker, Git, CI/CD, observability, system design

Tools: Claude Code, Cursor, Vercel

Languages: English (professional), Hindi and Tamil (native)

EDUCATION

B.Tech, Computer Science and Engineering (AI and Data Science) · SASTRA University · 2022 – 2026

CERTIFICATIONS AND PROGRAMS

Data Analytics & AI Launchpad Program (PwC Acceleration Centers India, 2025) · OWASP Top 10 (SecureFlag, 2026) · Supervised Machine Learning (DeepLearning.AI and Stanford, 2024) · Generative AI and Prompt Design in Vertex AI (Google Cloud, 2024)