Rohit Babu George

AI Engineer | Agentic AI, MCP & LLM Orchestration

rohitbabugeorge@gmail.com | rohit.simplewebsite.in | Kochi, Kerala
linkedin.com/in/rohit-babu-george | github.com/xrg360

Software engineer building agentic AI at Hexnode: MCP gateways, agent orchestration and guardrails for **Hexnode Synapse**, and an LLM documentation service for **Genie**, in **Python**, **Go** and **FastAPI** on **AWS Bedrock**.

EXPERIENCE

Hexnode (Mitsogo Inc.) – Kochi, Kerala — May 2025 – Present

Software Engineer – Hexnode AI Team — *Feb 2026 – Present*

Hexnode Synapse – agentic AI orchestration for IT & security, in pilot

- Co-developed Synapse's **agent orchestration** and **guardrail** components, turning plain-language requests into human-approved plans, plus agent **evals**.
- Built the event-driven **ingestor** that keeps the **context graph** of people, accounts and devices in sync in real time across Hexnode UEM, XDR, IdP and any system plugged in through **connectors**.
- Worked on the **governed execution layer** that authorizes, deduplicates and audits agent actions.

RLM Knowledge Service – grounding Genie & Synapse in Hexnode product docs

- Contributed to a **Recursive Language Model (RLM)** service over **1,600+** Hexnode UEM and XDR docs, where the LLM explores the documentation step by step for **platform-specific** answers.
- Worked across the **intent router**, **sub-LLM** extraction, query rewriting, **web-search fallback** and **source-integrity** checks so answers cite only docs actually read; served over **FastAPI** SSE on **AWS Bedrock**.
- Integrated it into **Genie** as a documentation tool, with **re-indexing** on every doc publish and **regression testing** against a curated QA suite.

MCP Gateways & Hexnode Genie – agentic AI across UEM, XDR & IdP

- Built Hexnode's **XDR** and **IdP MCP gateways** end to end and contributed to the UEM gateway (**FastMCP**, **FastAPI**, **Pydantic AI**), powering **Genie** across all three portals.
- Generated MCP tools from **OpenAPI** specs with **least-privilege access controls**, a read-only mode and secure **multi-tenant auth**.
- Built **PII redaction** for LLM traffic and a **cryptographically verified confirmation** step before destructive actions.
- Wrote a **40-case guardrail eval suite** in **pydantic-evals** (scope, confirmation, prompt injection).
- Added **OpenTelemetry** tracing in **Jaeger**: per-turn, model and tool-call spans with token and cost usage, and audit spans for destructive actions.

Software Engineer – UEM — *May 2025 – Feb 2026*

- Shipped Hexnode UEM (Windows, server-side) and MDM app features and fixes in **Django, Angular, PostgreSQL**.

PROJECTS

AI-Driven Smart Fire Evacuation System | *IEEE ICSCC 2025 publication, co-author* | GitHub — 2025

- Real-time A* evacuation routing over live sensor and indoor-positioning data, re-planning around fire.

TECHNICAL SKILLS

AI & Agents	RLM, MCP (FastMCP), Pydantic AI, guardrails, pydantic-evals, AWS Bedrock
Backend & Data	Python, Go, FastAPI, Django, Node.js, PostgreSQL, Apache AGE, MongoDB, NATS JetStream
Observability & Infra	OpenTelemetry, Jaeger, Prometheus, Docker, AWS, GCP, Git, CI/CD
Web	TypeScript, JavaScript, React, Next.js, Angular

EDUCATION

Muthoot Institute of Technology and Science — Kochi, Kerala

B.Tech in Computer Science and Engineering (CGPA: 8.61) — *Nov 2021 – May 2025*

Leadership: IEEE CS, IEEE SB MITS Chairperson (10+ events) | GDSC MITS AI & ML Lead, then App Dev Lead