

SAYERI BISWAS

AGENTIC AI ENGINEER | MULTI-AGENT SYSTEMS | LANGCHAIN | LANGGRAPH | MCP |
RAG | AZURE | PYTHON

Kolkata, West Bengal, India | +91 9836139228 | sayeri.techsec@gmail.com | linkedin.com/in/sayeribiswas96

PROFESSIONAL SUMMARY

Agentic AI Engineer with nearly 5 years of enterprise engineering experience at Infosys, building LLM-powered applications, multi-agent systems, and AI-driven workflow automation. Hands-on experience with LangChain, LangGraph, MCP, RAG, Python, FastAPI, Microsoft Azure, Kubernetes, and Docker. Experienced in agent orchestration, state management, conditional routing, sequential/parallel workflows, planning/replanning, tool/function calling, AI memory, human-in-the-loop controls, evaluation, observability, guardrails, and production deployment. Built an enterprise EDI AI Assistant / Digital Brain supporting EDI SDLC workflows and enterprise knowledge retrieval, reducing manual effort by 76%.

TECHNICAL SKILLS

Agentic AI & LLM Engineering: Agentic AI, AI Agents, Multi-Agent Systems, Multi-Agent Architecture, LangChain, LangGraph, Agent Orchestration, Agent State Management, Conditional Routing, Sequential/Parallel Workflows, Planning/Replanning, Agent Loops, Failure Recovery, Tool Nodes, Tool Calling, Function Calling, AI Memory, Human-in-the-Loop, Structured Outputs, Context Engineering, Prompt Engineering, Prompt/Model Versioning, Regression Testing

MCP & RAG: Model Context Protocol (MCP), MCP Servers, MCP Clients, Custom MCP Tools, Tool Discovery, Tool Integration, Tool Permissions/Authorization, REST APIs, Enterprise API Integration, Database Integration, Retrieval-Augmented Generation (RAG), Embeddings, Vector Databases, Semantic Search, Hybrid Retrieval, Metadata Filtering, Reranking, Query Transformation, Document Processing, Document Chunking, Retrieval Evaluation, Contextual Grounding, RAG Security, RAG Poisoning

Cloud, Platform & Backend: Microsoft Azure, Azure OpenAI, Azure AI Search, Azure Functions, Azure Storage, Azure Key Vault, Azure Monitor/Application Insights, Azure Container Registry, Azure Kubernetes Service (AKS), Kubernetes, Docker, Helm, Git, Jenkins, CI/CD, Octopus Deploy, Python, Async Python, FastAPI, JSON, Pydantic, SQL, Exception Handling, Retries, Timeouts, Input Validation, Logging, Testing, Production Deployment, Production Support

Evaluation, Observability & Security: AI/LLM Evaluation, Agent Evaluation, Langfuse, OpenTelemetry, Tracing, Metrics, Structured Logging, Tool-Call Observability, Prompt Injection, Indirect Prompt Injection, Jailbreak Mitigation, Tool Abuse Controls, Agent Authorization, Data Leakage Prevention, AI Guardrails, Sandboxed Execution, OWASP LLM Security, MITRE ATLAS

Enterprise Integration: Healthcare EDI, IBM Transformation Extender (ITX/WTX), ANSI X12, 834 Enrollment, 837 Professional Claims, 837 Institutional Claims, B2B Integration, XML, XSD, Flat Files

PROFESSIONAL EXPERIENCE

Technology Analyst | Infosys Limited

January 2022 - Present

- Built an enterprise EDI AI Assistant / Digital Brain supporting EDI SDLC workflows and enterprise knowledge retrieval using LangChain/LangGraph multi-agent orchestration, MCP-based tool integration, and workflow execution.
- Designed multi-agent workflows with specialized agents, shared context, persistent workflow state, conditional routing, tool nodes, planning/replanning, controlled multi-step execution, and human-in-the-loop approval points.
- Built and integrated MCP-based tooling, including MCP servers/clients and custom tools, connecting agents with enterprise tools, REST APIs, databases, data sources, and enterprise systems; applied tool permissions and authorization checks.
- Built enterprise RAG pipelines covering document processing and chunking, embeddings, vector search, semantic/hybrid retrieval, metadata filtering, reranking, contextual grounding, and retrieval evaluation.
- Developed AI application services using Python and FastAPI with request/input validation, structured outputs, asynchronous processing, exception handling, retries, timeouts, and API error handling.
- Implemented guardrails, validation, authorization controls, and human-in-the-loop approvals; applied controls for prompt injection, indirect prompt injection, jailbreak risks, RAG security, RAG poisoning, tool abuse, and sensitive-data handling.
- Established AI observability and evaluation across requests, retrieved context, model responses, agent/tool calls, approvals, latency, failures, and workflow outcomes using structured logging, metrics, tracing, Langfuse, OpenTelemetry, and regression scenarios.
- Designed, deployed, and maintained enterprise AI workloads using Microsoft Azure, Kubernetes, Docker, and CI/CD workflows, including containerized deployment, configuration/secrets management, monitoring, and production support.
- Automated enterprise request processing using LLM-based classification, extraction, summarization, and workflow automation, reducing manual effort by 76%.

AWARD

- Infosys INSTA Award** - Outstanding project contributions

CERTIFICATIONS

- Infosys Certified Agentic AI Professional
- Infosys Certified Python Associate

EDUCATION

Bachelor of Technology (B.Tech), Electrical Engineering - 2020 | RCC Institute of Information Technology