NISHANTH VEDURUVADA

AI Platform Architect

Agentic Platforms • AI Governance • Enterprise AI Modernization • Zero Trust Architecture

Hyderabad, India | +91 9010244874 | nishanth.themaster@gmail.com | linkedin.com/in/nish-ved | nishved.com

PROFESSIONAL SUMMARY

AI Platform Architect with 9+ years across platform, solution and cloud architecture and application security, targeting Principal and Enterprise Architect roles. I build the governance layer that lets autonomous systems ship inside regulated enterprises — reusable architecture domain teams inherit rather than rebuild. Currently AI Engineer Advisor at NTT DATA, leading architecture and technical governance for 8–10 enterprise AI modernization programs in the Syntphony product ecosystem, with a team of engineers and data scientists. Previously sole architect of the AI Trust Fabric for a national-scale insurance data ecosystem — work registered as an industrial design with the Government of India. Depth spans Agentic AI and multi-agent systems, Model Context Protocol (MCP) and Agent-to-Agent (A2A) tool protocols, Retrieval-Augmented Generation (RAG), Large Language Model (LLM) platforms, AI Governance, and NIST 800-207 Zero Trust Architecture, applied in regulated insurance, telecommunications and energy.

SELECTED ACHIEVEMENTS

- **Registered industrial design, Government of India.** Sole architect of the AI Trust Fabric — a NIST 800-207 Zero Trust framework with adaptive trust scoring and AI agent governance for a national-scale insurance data ecosystem — registered as Design No. 485611-001.
- **Peer-reviewed publication on AI agent security.** Co-author, *MCP Guardian: A Security-First Layer for Safeguarding MCP-Based AI Systems* — independent research proposing authentication, rate limiting and audit for Model Context Protocol tool calls.
- **Reference architecture for a reusable multi-agent platform.** Standardised MCP for tool integration and A2A for cross-domain agent collaboration, so domain teams inherit per-agent identity, audit and approval controls rather than rebuilding governance per engagement.

CORE COMPETENCIES

Enterprise Architecture · Solution Architecture · Cloud Architecture · Agentic AI · Generative AI · Retrieval-Augmented Generation (RAG) · AI Governance · Zero Trust Architecture · Cybersecurity · Technical Leadership

PROFESSIONAL EXPERIENCE

NTT DATA

Dec 2025 – Present

AI Engineer Advisor

Architecture and technical governance for AI modernization across NTT DATA's Syntphony ecosystem — Syntphony AI, Open Telecom Networks, Insurance Cloud Migration, Stations, and Commerce & Payments.

- **AI Governance Controls:** Established per-agent OAuth2 identity, full tool-call audit logging, configurable rate limits, action-scope enforcement, and a human-in-the-loop approval gateway for high-risk actions — inherited automatically by every domain agent on the platform.
- **Enterprise Retrieval Architecture:** Designed a dual-path knowledge assistant separating live analytics from indexed content: semantic-model queries with row-level security passed through as the calling user, alongside permission-scoped document retrieval, routed by a query classifier. Metric values are never embedded, so answers cannot go stale.
- **Legacy Modernization:** Architected an MCP-based code intelligence system over mainframe COBOL and JCL estates for insurance cloud migration, built on a structure-aware parser and static dependency graph. The model queries the live codebase through MCP tools rather than an embedded index, so every answer cites program, paragraph and line.
- **Technical Leadership:** Lead architecture reviews, decision records and trade-off analysis for the team; own enterprise AI architecture standards, technical strategy, stakeholder alignment and mentoring.

Levo.ai

Jan 2025 – Dec 2025

AI Enterprise Architect

Client: national-scale insurance data ecosystem (India)

Sole architect of the AI Trust Fabric for a national-scale insurance data ecosystem aggregating records from across the country's insurance industry, under national insurance-regulator oversight and data-localisation requirements.

- **Zero Trust Architecture:** Designed the full NIST 800-207 structure — policy administration, decision, enforcement and information points as separate concerns — with enforcement deployed as an API gateway intercept so every call, human or agent, traverses it.
- **Adaptive Trust Engine:** Replaced binary allow/deny with continuous trust scoring across identity confidence, device posture, behavioural baseline, data classification and context, driving allow / step-up-authentication / deny decisions with thresholds configurable per data class.
- **AI Agent Identity & Governance:** Gave agents their own workload identity rather than borrowed user credentials, with action-scope enforcement, per-agent rate limiting, prompt-injection detection, full decision audit, and human escalation above a risk threshold.
- **Offline AI Capability:** Architected fully offline inference with Ollama to satisfy no-internet-egress environments — a hard constraint that would otherwise have blocked the entire governance layer.

Arcstream Technologies
Aug 2022 – Jan 2025

Technical Security Lead

- **Enterprise Security Modernization:** Led Zero Trust network segmentation and a SASE migration covering 5,000+ users, replacing perimeter-based access with identity-centric controls.
- **Secure Delivery:** Hardened CI/CD pipelines and established architecture governance across engineering teams.

Reezanorp Technologies
Dec 2016 – Jul 2022

Senior Software Engineer

- **Applied ML & Data Engineering:** Built machine learning, analytics, computer vision, ETL and enterprise automation systems in Python — the engineering foundation underneath the later architecture work.

PUBLICATIONS & INTELLECTUAL PROPERTY

MCP Guardian: A Security-First Layer for Safeguarding MCP-Based AI Systems

Computer Science & Information Technology (CS&IT), Vol.15 No.9, pp.107–121, 2025 · DOI 10.5121/csit.2025.150908

Middleware for the Model Context Protocol adding authentication, per-token rate limiting, WAF-style scanning of tool calls and request logging, without modifying individual MCP servers. Evaluated at roughly 3–4 ms median latency overhead.

AI Trust Fabric — Secure Insurance Data Management Device

Registered Design No. 485611-001, Government of India · Co-inventor

The Zero Trust and AI governance architecture designed for a national-scale insurance data ecosystem — NIST 800-207 policy separation, adaptive trust evaluation, identity-centric controls and secure data access mechanisms.

TECHNICAL SKILLS

AI & Machine Learning: Agentic AI, Multi-Agent Systems, Generative AI (GenAI), Large Language Models (LLM), Retrieval-Augmented Generation (RAG), Machine Learning, Predictive Analytics, Computer Vision, Conversational AI, Semantic Search, Prompt Engineering, LLMOps, AI Evaluation

AI Frameworks & Protocols: Model Context Protocol (MCP), FastMCP, Agent-to-Agent (A2A), CrewAI, LangGraph, LangChain, AutoGen, Semantic Kernel, Tool Calling, Human-in-the-Loop, Vector Databases, ChromaDB, Azure AI Search

AI Platforms: Azure OpenAI, Azure AI Foundry, OpenAI, Anthropic Claude, Ollama, Google Vertex AI, GPT-4o

Security & Governance: Zero Trust Architecture, NIST 800-207, Policy Administration/Decision/Enforcement/Information Points (PAP/PDP/PEP/PIP), Identity and Access Management (IAM), Microsoft Entra ID, OAuth 2.0, OpenID Connect (OIDC), Multi-Factor Authentication (MFA), Zero Trust Network Access (ZTNA), Secure Access Service Edge (SASE), Data Loss Prevention (DLP), API Security, AI Governance, Explainability, Audit & Compliance, Row-Level Security (RLS)

Cloud & Platform: Microsoft Azure, Kubernetes (AKS), Docker, Microservices, Event-Driven Architecture, Apache Kafka, Azure Service Bus, Azure API Management, Azure Logic Apps, Cosmos DB, Microsoft Fabric, Power BI, Microsoft Graph, OpenTelemetry, CI/CD, DevSecOps

Engineering: Python, FastAPI, REST APIs, GraphQL, SQL, Git, Legacy Modernization, COBOL/JCL analysis, ETL, Solution Architecture, Enterprise Architecture, Technical Leadership, Mentoring, Stakeholder Management

EDUCATION

Bachelor of Technology (B.Tech), Electronics & Communication Engineering — Jawaharlal Nehru Technological University (JNTU), India