

Amrik Singh Khalsa

AI Agent Systems & Software Architect

Bangalore, India • singhamrikkhalsa@gmail.com • amriksinghkhalsa.com • linkedin.com/in/amriksinghkhalsa • github.com/amriksingh0786

SUMMARY

Software architect specializing in AI agent systems: multi-agent orchestration, MCP and A2A protocol runtimes, agent identity, and the security gates that make executable agent skills safe to distribute across an engineering organization. Five years building and leading full-stack platforms, including a fintech system that moved \$5M+ in equity transactions.

EXPERIENCE

Okta (Auth0)

Senior Software Engineer

Oct 2025 to Present

Bangalore, India

- ♦ **AI Agent Security & Governance:** Own the CI security gates for an org-wide marketplace distributing 170+ executable AI agent skills to every engineering team. Shipped 3 merged gates (LLM-backed security scanner, static-analysis pre-commit hook, duplicate-skill gate) plus the Terraform module and GitHub OIDC-federated IAM roles supplying short-lived model credentials with no long-lived secrets.
- ♦ **Multi-Agent Systems:** Architected an orchestrator, analyst and synthesizer agent fleet that root-causes production escalations with cited evidence across 4 parallel subagents; root-caused 11+ escalations end to end and promoted the system from a personal skill to an org-wide plugin.
- ♦ **Agent Platform Engineering:** Delivered 6 agent-platform proofs of concept end to end: an A2A protocol runtime (1,200+ tests green), MCP servers, agent memory with retrieval grounding on AWS Bedrock AgentCore, and agent context and cost observability.
- ♦ **AI Knowledge Agent (RAG & pgvector):** Architected a GenAI support agent using Retrieval-Augmented Generation and pgvector for high-dimensional vector search; automated ingestion of 2,000+ technical articles, cutting internal query resolution time by 40%.
- ♦ **Notification Service:** Designed and deployed a high-availability notification microservice for Private Cloud customers, with secure event-driven pipelines guaranteeing delivery of critical security patches and system alerts.
- ♦ **Delivery:** 30+ PRs merged and 30+ reviewed across platform and security repositories; 80+ architecture and research documents published.

Incentiv

Founding Engineer & Tech Lead

Apr 2024 to Jun 2025

Bangalore, India

- ♦ **Leadership & Product Ownership:** Led a cross-functional engineering team delivering Incentiv's core platform, driving \$5M+ in ESOP liquidity; onboarded 30+ startups and 200+ investors in 6 months.
- ♦ **AI Agent (Atlas AI):** Built and deployed an autonomous agent (LangChain, Puppeteer, LLMs) for research, automation and content generation, boosting team efficiency by 50%.
- ♦ **System Design & Architecture:** Designed scalable, low-latency systems handling 10K+ equity transactions per month, with secure document pipelines and investor-startup workflows.
- ♦ **Full-Stack Engineering:** Architected shared service layers with NestJS and Prisma, cutting response times by 25%; delivered performant UIs with Next.js, Framer Motion and Tailwind for 35% faster page loads.
- ♦ **Automation & Security:** Built dynamic EditorJS templates and an in-app investor update engine, cutting content turnaround by 80% and lifting response rates by 40%; implemented AES-256, JWT, OAuth2, RBAC and 2FA aligned to OWASP Top 10 and GDPR.

Augmento Labs Pvt Ltd

Software Engineer to Frontend Lead

Jun 2021 to Apr 2024

Bangalore, India

- ♦ **Frontend Leadership & System Design:** Led the frontend team and architected scalable micro-frontend systems, reducing infrastructure costs through optimized resource allocation.
- ♦ **Shared Component & Service Layer:** Built a component library and shared service layer used across 6+ micro-frontends, boosting performance by 34% and cutting new microservice development time by 40%.

- ✦ **Cloud Migration:** Migrated the logging component from SQL to Azure Table Storage, improving performance by 44% and reducing storage costs by 24%.

OPEN SOURCE

NVIDIA NeMo Agent Toolkit *(agent framework & fine-tuning)*

PRs [#2323](#), [#2329](#), [#2330](#), all merged

Fixed tool-call linkage in fine-tuning trajectories: the LangChain parser wrote the integer 0 as the tool_call_id of every tool message, so no tool result matched the call it answered. Fixed the same defect in both training backends: the OpenPipe ART adapter now maps tool results to the tool role, and the NeMo Customizer DPO path keeps tool_call_id and name.

20 unit tests · +436 / -9

Microsoft Agent Governance Toolkit *(agent policy & audit runtime)*

PRs [#4280](#), [#4164](#), [#4175](#), [#3783](#), all merged

Made tool-output secret redaction configurable through a validated, fail-closed secretPatterns policy key, and doubled the default set from 7 to 14 credential formats. Added decision evidence to the hash-chained, tamper-evident audit log and closed a secret-path leak found in review. Fixed audit-log rollover that broke verification past 10,000 entries, and bounded TypeScript kill-switch callbacks with a configurable timeout.

71 unit tests · +2,519 / -90

Warp *(Rust terminal)*

PR [#9503](#), merged

Executable shell scripts opened from a file:// URL now run in the terminal instead of opening in the editor, through a pure classification helper gated on the user-execute bit plus extension or shebang on Unix, and extension on Windows.

13 unit tests · +312 / -4

SKILLS

AI & Agents	Claude Agent SDK, Multi-Agent Orchestration, MCP (Model Context Protocol), A2A, LangChain, LangGraph, RAG, pgvector, AWS Bedrock, AgentCore, Agent Security, Prompt Injection Defense, Eval Harnesses
Languages	TypeScript, JavaScript, Python, Go, Rust, C#, SQL
Frontend	React, Next.js, Angular, Redux, TailwindCSS, shadcn/ui, Material UI, Framer Motion
Backend & Data	Node.js, NestJS, Express, .NET, Prisma, Drizzle, PostgreSQL, Redis, Azure Table Storage
Cloud & DevOps	AWS, Azure, GCP, Terraform, Docker, GitHub Actions, GitHub OIDC, Vercel, Traefik
Practices	System Design, Micro-frontends, OAuth2 / JWT / OIDC, RBAC, AES-256, OWASP Top 10, GDPR

EDUCATION

B.Tech, Computer Science

2017 to 2021

Shri Vaishnav Vidyapeeth Vishwavidyalaya (SVVV), Indore

ACHIEVEMENTS

3x Employee of the Month, Augmento Labs

President, PRAYATNA (non-profit)

Founder & President, CodeChef SVVV Chapter

5 Star HackerRank

Best Project Award, College Hackathon

Member, ACM