Gautham Vijayaraj

Tempe, AZ | gvofficial99@gmail.com | +1 (602) 247-0511 | gauthiii.github.io
linkedin.com/in/gautham-vijayaraj | github.com/gauthiii

Executive Summary

AI Security Engineer specializing in AI governance, secure agentic systems, and enterprise AI transformation. Developed AI governance and security frameworks for Blue Cross Blue Shield and Aspire Health by translating enterprise transformation initiatives into AI capabilities and mapping those capabilities to risks and controls. Experienced with ServiceNow AI Control Tower and AI Risk & Compliance, and comfortable working with the Microsoft Azure Foundry stack. Designed model-agnostic AI workflows, implemented context caching, reduced LLM pipeline costs, and mitigated OWASP-listed LLM vulnerabilities. Built agentic applications using MCP, A2A protocols, RAG, LangChain, LangGraph, and AWS Bedrock, supported by Python, FastAPI, React.js, Neo4j, and Docker. Combined a cybersecurity background with ServiceNow certifications in platform administration, application development, and asset management to support AI risk assessment, secure architecture, and enterprise automation.

Education

Arizona State University, MS in Computer Science (Cybersecurity) Aug 2023 – May 2025

SRM Institute of Science & Technology, B.Tech in Computer Science Engineering July 2017 – May 2021

Experience

AI Security Engineer, Santan Intellect Inc. – Ashburn, VA May 2026 – Present

- Collaborated with Blue Cross Blue Shield and Aspire Health to translate enterprise transformation initiatives into AI capabilities
- Mapped each client's AI capabilities to risks and controls and developed an AI governance and security framework for each organization
- Architected and implemented AI governance workflows on ServiceNow AI Control Tower and AI Risk & Compliance (AIRC), building risk classification, impact assessment, and playbook approval pipelines aligned to EU AI Act and NIST AI RMF frameworks for a healthcare patient portal
- Configured ServiceNow AI Agent Studio agents with least-privilege ACL-based custom roles, and built Agent-to-Agent (A2A) OAuth authentication flows using FastAPI as a secure proxy layer
- Diagnosed and resolved gaps in AICT/AIRC automation logic, including Advanced Risk Assessment migration, RAM configuration, and Post Assessment Actions to enable end-to-end risk score roll-up and automated risk/control mapping
- Produced executive-facing deliverables, including a stakeholder demo narrative and supporting materials, translating technical AI governance controls into a clear risk-to-compliance story for healthcare data stakeholders
- Architected and designed a Digital Twin solution integrating ArcGIS with ServiceNow to provide real-time geospatial visualization of telecom and enterprise infrastructure, enabling centralized monitoring, asset correlation, and operational intelligence across distributed environments
- Engineered geospatial workflows for TNI (Telecommunications Network Inventory) Mapping and Field Service Management (FSM), enabling automated work order orchestration, technician dispatching, route-based field operations, and infrastructure lifecycle tracking through ArcGIS and ServiceNow integration
- Designed and implemented integrated Vulnerability Response and Security Incident Response Management workflows within the Digital Twin ecosystem, correlating security events, vulnerable assets, network topology, and geographic impact zones to improve threat visibility, incident prioritization, and coordinated remediation activities across operational and security teams

AI Engineer, Santan Intellect Inc. – Ashburn, VA Nov 2025 – Apr 2026

- Developed an agentic software solution to automate the end-to-end information security management (ISM) system lifecycle

- Implemented context caching to reuse LLM context across AI workflows
- Reduced LLM pipeline costs from $130 to $40, a reduction of approximately 69%
- Designed model-agnostic AI workflows to support integration with multiple LLMs
- Mitigated OWASP-listed LLM vulnerabilities in AI workflows
- Implemented a Model Context Protocol (MCP) server to integrate, initialize, and execute Neo4j Cypher queries using Gemini LLM, enabling natural language querying and intelligent graph-based insights
- Orchestrated an Agent-to-Agent (A2A) protocol to coordinate a multi-agent workflow of 70+ AI agents
- Developed and integrated secure authentication services using AWS Cognito, implementing multi-factor authentication (MFA) and identity management across microservice-based architectures
- Enhanced React-based user interfaces to visualize AI-driven insights with a focus on usability and performance
- Applied ServiceNow fundamentals and system administration practices to manage records, configure Now Assist, build applications in App Studio, and maintain core modules including CMDB, CSDM, and ITSM processes

AI Engineer, Reveille Technologies, Inc. – Charlotte, NC July 2025 – Oct - 2025

- Developed a RAG-based onboarding chatbot leveraging AWS Bedrock, LangChain, and FAISS for contextual retrieval and dynamic knowledge integration, enhancing employee onboarding and internal query resolution
- Collaborated in code reviews, test coverage improvement, and CI/CD pipelines (GitHub Actions, Docker)

Software Engineer Intern, HCLTech, – Chennai, India May 2024 – Aug 2024

- Built Spring Boot microservices to to manage healthcare-related queries using a RAG-based pipeline
- Developed NLP-driven interfaces powered by Gen AI and LangChain, enabling scalable and intelligent query understanding across distributed healthcare systems ensuring secure retrieval and context-aware responses

Assistant System Engineer, Tata Consultancy Services, – Chennai, India June 2021 – Nov 2022

- Developed financial analytics dashboards with React.js, TypeScript, Java (Spring Boot), and MySQL
- Improved system reliability and scalability by implementing optimized database queries and modular APIs

Projects [gauthiii.github.io/projects.html]

Product Documentation MCP Server (github.com/gauthiii/ai_service_now_docs)

- Built an MCP (Model Context Protocol) server exposing ServiceNow's official AI Implementation and GRC documentation (500+ subtopics) as searchable, LLM-readable context via index, search, and fetch tools
- Designed a PDF-to-markdown extraction pipeline that splits large source PDFs into bookmark-preserving chunks and restructures them into a document/topic/subtopic hierarchy for efficient semantic retrieval

GlobalStocks : AI-Assisted Portfolio Dashboard (github.com/gauthiii/globalStocks)

- Built a React + Vite dashboard for tracking US and India stocks/funds with a FastAPI backend that orchestrates Claude and OpenAI agents (with live web search) to generate per-stock research notes on demand
- Engineered a market-aware cron scanner detecting trailing-window highs/lows (1 day to 1 month) across a multi-instrument watchlist, with automated Telegram alerts gated to live NSE/US market hours

InboxPulse : Email Intelligence Dashboard (github.com/gauthiii/inboxPulse)

- Developed a privacy-first, multi-account Gmail dashboard (Node.js/Express + React) using a read-only OAuth scope and a hybrid rules + LLM pipeline to classify mail into nine priority categories
- Implemented AES-256-GCM token encryption, server-side HTML sanitization, and local-only SQLite storage to ensure strict data privacy with no third-party data retention

Microservice Analyzer : AI Codebase Analysis Agent (github.com/gauthiii/microservice_analyzer)

- Built an AI agent using Google Gemini to recursively scan and analyze an entire project directory, automating codebase comprehension and structural review

Multi-Agent Orchestration with A2A Protocol and MCP Servers (github.com/gauthiii/a2aProjects)

- Developed an integrated multi-agent orchestration framework using the A2A protocol and Model Context Protocol (MCP) servers for cross-domain automation through asynchronous LLM-driven coordination
- Enabled seamless agent-to-agent (A2A) communication between Reddit, Flights, Airbnb, and Finance MCP servers to automate market analysis, trip planning, and real-time report generation with multi-model LLM

Multi-Server MCP Orchestration with External and Custom Tools (github.com/gauthiii/mcpServer)

- Built an LLM-driven orchestration system integrating multiple MCP servers (Playwright, Airbnb, DuckDuckGo, OpenWeather, Gmail) to automate browsing, booking, weather retrieval, and email parsing

Agentic Research Workflow with Reflective AI Agents (github.com/gauthiii/agenticAIProjects)

- Designed a multi-agent research system using OpenAI and Claude LLMs that autonomously selects and executes tools (Arxiv, Tavily) to generate structured research reports that were refined using a reflection-feedback loop

Certifications

ServiceNow Certified System Administrator (CSA)

- Validated expertise in ServiceNow platform administration, including user management, access controls, workflows, data models, and core ITSM configurations
- Verify at: https://www.credly.com/badges/bec551af-e919-41c8-896c-afb7ab56a2be/public_url

ServiceNow Certified Application Developer (CAD)

- Demonstrated proficiency in developing scoped applications using App Engine Studio, scripting, Flow Designer, and advanced ServiceNow platform capabilities
- Verify at: https://www.credly.com/badges/3d4d634b-dbc3-4e15-869b-59f6b1511619/public_url

ServiceNow Certified Implementation Specialist – Data Foundations (CMDB & CSDM)

- Specialized in ServiceNow CMDB architecture, Common Service Data Model (CSDM), discovery, data normalization, and service mapping best practices
- Verify at: https://www.credly.com/badges/7fbc07a1-fc83-4e6a-9445-6d5a28bf4d19/public_url

ServiceNow Certified Implementation Specialist – Hardware Asset Management (HAM)

- Specialized in ServiceNow lifecycle management, asset tracking, compliance, and cost optimization for enterprise IT hardware assets
- Verify at: https://www.credly.com/badges/04fcd114-b6fc-454a-aefc-69eb1dcf5510/public_url

ServiceNow Certified Implementation Specialist – Software Asset Management (SAM)

- Specialized in ServiceNow lifecycle management, asset tracking, compliance, and cost optimization for enterprise IT software assets
- Verify at: https://www.credly.com/badges/01bef89d-f609-4d26-b838-ba3565283906/public_url

Google Cybersecurity Professional Certificate

- Built foundational skills in cybersecurity principles, threat detection, incident response, IAM, SIEM tools, and security best practices aligned with industry standards
- Verify at: https://www.coursera.org/account/accomplishments/professional-cert/Q9ZGGTT9P87L

IBM Generative AI Engineering Professional Certificate

- Covered end-to-end generative AI concepts including foundation models, prompt engineering, LLM fine-tuning, AI pipelines, and real-world enterprise use cases
- Verify at: https://www.coursera.org/account/accomplishments/professional-cert/QI0194CDQKBM

Skills and Technologies

AI Security & Governance: AI Capability Risk and Control Mapping, AI Governance and Security Frameworks, AI Risk Assessment, OWASP LLM Vulnerability Mitigation

ServiceNow: AI Control Tower (AICT), AI Risk & Compliance (AIRC), AI Agent Studio, Flow Designer, App Engine Studio, CMDB/CSDM, ITSM, HAM/SAM, Vulnerability Response, Security Incident Response, ACLs & Role-Based Access, Table API, Scripted REST APIs

Agentic AI: Claude Code, Codex, MCP, A2A Protocol, RAG Pipelines, Multi-Agent Orchestration, LangChain, LangGraph, Google ADK, Retrieval Augmented Generation (RAG)

Generative AI: Context Caching, LLM Cost Optimization, Model-Agnostic AI Workflows, Hugging Face, Keras, Transformers, Prompt Engineering, Fine-Tuning, TensorFlow, Deep Learning

Cloud & DevOps: Microsoft Azure Foundry, AWS Bedrock, Lambda, Step Functions, EC2, ECR, Docker, GitHub, GitHub Actions, CI/CD

Software Development: React.js, Python, TypeScript, SQL, Spring Boot, FastAPI, Neo4j, REST API, System Design

Geospatial: ArcGIS, ArcGIS Feature Layers, Geospatial Data Modeling