PRASIDDHA PAUDEL

AI Engineer | Secure Backend Systems | LLM Integration & AI Security

Broomfield, CO (Open to Relocate) | (720) 299-8934 | prasiddhapaudel9@gmail.com

GitHub: [add link] | linkedin.com/in/prasiddhapaudel | Authorized to work in the US (OPT/EAD)

PROFESSIONAL SUMMARY

Backend and security-focused software engineer with 4+ years of experience building secure RESTful APIs and production systems in Java/Spring Boot and Python/FastAPI, now specialized in LLM integration and AI security. Builds and ships production AI security tooling on AWS — including prompt injection defense, secure LLM gateways, and AI-assisted security operations — grounded in application security practice (CompTIA Security+, ISC2 CC, OWASP LLM Top 10).

AI ENGINEERING PROJECTS (LIVE ON AWS)

Secure LLM API Gateway | *Java 17 · Spring Boot 3 · Redis · PostgreSQL · Docker · AWS EB · OpenAI · Anthropic* | [GitHub link]

- Built a production-grade Spring Boot 3 API gateway that proxies OpenAI and Anthropic API calls through a 5-layer security pipeline: JWT authentication, Redis rate limiting (20 req/min), prompt injection detection, LLM proxying, and output sanitisation — addressing OWASP LLM Top 10 #01 and #05.
- Deployed on AWS Elastic Beanstalk with RDS PostgreSQL 16 and ElastiCache Redis 7; Docker image published to ECR. Every request audit-logged asynchronously to PostgreSQL with SHA-256 hashed prompts for privacy compliance.
- Implemented Strategy pattern for multi-provider routing (OpenAI + Anthropic) — adding a new LLM provider requires one new class with zero changes to gateway logic. Live at: llm-gateway-prod3.eba-fthxkeyz.us-east-1.elasticbeanstalk.com

SentinelAI — LLM-Powered Security Operations Platform | *Python · FastAPI · Claude API · SQLite · ReportLab · WebSocket · Docker · AWS EB* | [GitHub link]

- Built an AI-driven security operations platform combining red team (recon, vulnerability analysis) and blue team (log analysis, threat correlation) workflows powered by the Claude API, with real-time WebSocket streaming of security analysis to a live dashboard.
- Implemented a multi-log correlation engine that cross-references Apache, SSH, Nginx, and Windows Event logs to reconstruct complete attack chains — identifying same-IP attacks across multiple vectors — and generates downloadable PDF security reports via ReportLab.
- Covers OWASP API Security Top 10: API key authentication, rate limiting (120 req/min), CSP headers, input validation. 12 API endpoints live on AWS. Live at: sentinelai-prod.eba-3xqvpc6q.us-east-1.elasticbeanstalk.com

Vibe Code Security Auditor (In Progress) | *Python · FastAPI · Claude API · AST parsing · OWASP* | [GitHub link]

- AI-powered code security auditor that scans uploaded codebases or GitHub repositories for vulnerabilities, generates a 0–100 security score, and produces line-level findings with suggested fixes — targeting the critical gap of AI-generated code deployed without security review.

PROFESSIONAL EXPERIENCE

Software Engineer | Maulik Taranga Pvt. Ltd | Nepal (Remote) *Dec 2022 – Apr 2024*

- Designed and secured 10+ RESTful API endpoints with OAuth2 authentication and role-based access control — architecture directly applicable to securing LLM API integrations and AI service backends.
- Implemented OWASP Top 10 and NIST CSF secure coding practices, including input validation patterns relevant to prompt injection defense; reduced security defects by 40%.
- Built 15+ Java/Spring Boot backend enhancements; optimized MySQL queries improving data retrieval by 25%. Supported Jenkins CI/CD pipelines reducing post-release issues by 20%.
- Performed API security testing with Postman and Burp Suite, increasing pre-release defect detection by 30%.

Software QA Automation Engineer | Cedargate Technologies | Nepal *Mar 2021 – Oct 2022*

- Designed and built a QA automation framework from scratch using Java, Selenium WebDriver, TestNG, and SQL for healthcare web applications.
- Integrated automated test suites into Jenkins CI/CD pipelines enabling nightly regression testing; validated network traffic anomalies using Wireshark.

Software Engineer | Aasha Tech Pvt. Ltd | Nepal *Sep 2019 – Feb 2021*

- Developed Java Spring Boot backend and RESTful APIs for a university scholarship platform with OAuth 2.0 authentication, RBAC, and a React frontend.
- Applied Secure Development Lifecycle (SDL) practices including OWASP-aligned input validation and secure session management.

IT Support Specialist | Bupa Aged Care Homes | Sydney, Australia *Jan 2018 – Aug 2019*

- Delivered technical support to 200+ end users; managed Active Directory and group policies, improving onboarding efficiency by 30%. Supported Office 365 cloud migration.

TECHNICAL SKILLS

AI / LLM: LangChain, OpenAI API, Anthropic Claude API, RAG, ChromaDB, Pinecone, Prompt Injection Defense, OWASP LLM Top 10, HuggingFace, FastAPI

Languages: Java 17, Python 3.11, JavaScript (ES6+), TypeScript, PowerShell, Bash

Backend: Spring Boot 3.x, Spring Security, FastAPI, Flask, RESTful APIs, OAuth 2.0, JWT, Microservices, WebSockets

Cloud / DevOps: AWS (EB, ECR, RDS, ElastiCache, IAM, S3, EC2), GCP, OCI, Docker, Kubernetes, Jenkins, GitLab CI/CD

Security: Burp Suite, OWASP ZAP, Wireshark, Splunk, SAST/DAST, SonarQube, NIST CSF, ISO 27001, HIPAA

Databases: PostgreSQL, MySQL, SQLite, MongoDB, Redis, DynamoDB

Frontend: React, Node.js, Angular, TypeScript

EDUCATION

Master of Science in Computer Science *Expected December 2026*

Maharishi International University, Iowa, USA | Coursework: Algorithms, Advanced Software Development, Big Data, Cloud Computing

Bachelor of Science in Information Technology *July 2017*

University of Technology Sydney, Australia | Coursework: Cloud Computing, Software Architecture, Database Management, Web Services

CERTIFICATIONS

- CompTIA Security+ *Jan 2024*
- ISC2 Certified in Cybersecurity (CC) *Apr 2025*
- Google Cloud Cybersecurity Certificate *Sep 2025*
- TryHackMe SAL1 – Security Analyst Level 1 *2025*
- Oracle Cloud Infrastructure Certified Architect Associate *2024*
- Oracle Cloud Infrastructure MultiCloud Architect Professional *2024*
- Certified Cloud Associate (CCA) *2026*