

Chanakya Thotakura

Maryville, MO · chanikya1@icloud.com · linkedin.com/in/chanikya6163 · github.com/Chanikya5793

Summary

Software engineer shipping security-sensitive AI and cloud products across mobile, backend, and infrastructure. Built endpoint detection, encrypted apps, retrieval-backed copilots, and consumer threat monitoring with Python, TypeScript, React Native, Firebase, AWS, GCP, and Cloudflare.

Technical Skills

Security: Detection engineering, endpoint assurance, breach and dark-web monitoring, phishing/URL analysis, IAM, Signal E2EE
AI: RAG, MCP, Gemini/Vertex AI, embeddings, vector search, prompt-injection defense, structured outputs, evaluation
Cloud & Backend: AWS, GCP, Firebase, Cloudflare, Docker, FastAPI, REST, Cloud KMS, Secret Manager, SQLite
Languages & Frameworks: Python, TypeScript/JavaScript, Swift, Kotlin, SQL, React Native, React, GitHub Actions

Technical Experience

ControlForge Security | *Open-source security platform* Aug. 2026 to Present

- Released v0.1.0 of a Python platform that verifies endpoint controls and evaluates normalized events with version-controlled Sigma-style rules. Its CLI and FastAPI service return stable alert IDs, matched evidence, and investigation-ready reasons.
- Built stateful impossible-travel and sensitive-data-access detections alongside rules for encoded PowerShell, phishing, and off-workflow privilege grants. Read-only probes and an SQLite audit trail keep investigations predictable.
- Deployed the Dockerized API on AWS, stored signed release artifacts in S3, and published its operator surface through Cloudflare Pages. GitHub Actions runs strict typing, security analysis, packaging, and release checks.

Northwest Student Planner + RAG Copilot | *Graduate project, live web app* Jun. 2026 to Present

- Shipped web and Expo planner clients with encrypted offline storage. The public web app runs on GitHub Pages, while the authenticated FastAPI service runs on Cloud Run with Firebase Auth and Firestore.
- Built a user-scoped RAG copilot with Vertex AI, Gemini 2.5 Flash, UID-filtered vector search, and six read-only MCP tools. Per-user AES-256-GCM keys are wrapped by Cloud KMS; Firestore rules deny direct client access.
- Gemini cites retrieved records or abstains and returns a typed proposal. The app previews it and performs a revision-checked, idempotent write only after confirmation. A 30-query regression suite covers retrieval, citations, abstention, proposals, and user isolation.

ManaSplit | *Mobile product, TestFlight beta* Nov. 2025 to Present

- Distributed a React Native expense, messaging, and calling app through TestFlight and tested releases on physical iPhones. Native Swift and Kotlin modules support offline delivery; each linked device gets a Signal session with hardware-backed keys.
- Built an opt-in Security Center for breach, dark-web, infostealer, phishing, and account-takeover risk. Identities use AES-256-GCM envelope encryption, Cloud KMS-wrapped per-user keys, scoped blind indexes, and Secret Manager credentials.
- Combined HIBP, Flare, Web Risk, DNS/RDAP, TLS, and certificate-transparency signals with k-anonymous password checks and deterministic scoring. Evidence-bounded AI explains findings without receiving raw passwords, tokens, or provider secrets.

Machine Learning Intern | *AIMERS, AI engineering internship* Mar. 2025 to Aug. 2025

- Built and deployed on AWS a Python voice-assistant pipeline connecting speech recognition, supervised intent classification, secured database retrieval, and text-to-speech.
- Locked down the AWS-hosted database path with least-privilege roles, encryption in transit and at rest, managed secrets, parameterized SQL, query allowlists, schema validation, output redaction, and audit logging.
- Defended the speech and frontend boundary against prompt injection, jailbreaks, replay, and abuse with transcript normalization, rate limits, intent allowlists, bounded tool access, secure sessions, output validation, and safe refusals.

Education & Certifications

Northwest Missouri State University | *M.S., Applied Computer Science* Maryville, MO

- Coursework: Cybersecurity & Information Security Management, Advanced Database Systems, Web Applications.

V.R. Siddhartha Engineering College | *B.Tech., Computer Science & Engineering* Vijayawada, India

Certifications: Google Cloud Associate Cloud Engineer; Cisco Networking Academy: CyberOps Associate, Cybersecurity Essentials, CCNA Enterprise Networking, Security, and Automation, and CCNA Switching, Routing, and Wireless Essentials.