Nikhil Kumar

Hyderabad, India | Open to relocation
nikhilnkup@gmail.com | linkedin.com/in/nkupa | github.com/Nikhil-K-u | nikhil-k-u.github.io

Summary

Software engineer working on application and AI security, with 2+ years of Java and Python at KloudGin (full time since Aug 2025, after a year-long internship). Designed a server-side Backend-for-Frontend that keeps OAuth tokens, API keys and internal endpoints out of the browser; built LLM-agent tooling that vets every URL for phishing and scam signals and treats web content as untrusted input. Google Cybersecurity and Microsoft Security, Compliance & Identity certified.

Technical Skills

AppSec & Identity: Secure API Design, OAuth 2.0 / Bearer Tokens, Session Management, Secrets Management, CORS, Presigned-URL Access Control
AI Security: Prompt-Injection Screening, Untrusted-Input Handling for LLM Agents, LLM-Based Phishing / URL Risk Triage
Security Foundations: NIST CSF, Incident Response, SIEM Concepts, Network Security, Linux CLI & SQL Labs (Google Cybersecurity, SC-900)
Engineering: Python, Java, SQL, Bash, Linux, REST APIs, Spring Boot, Microservices, FastAPI, AWS (EC2, S3, SNS, SES), Azure, Git, CI/CD

Experience

KloudGin Inc. – Enterprise Field-Service & Asset Management SaaS Hyderabad, India
Associate Software Engineer *Mar 2026 – Present*

- **Reliable concurrent processing:** Engineered a multithreaded Java ingestion engine (hundreds of thousands of records through the KloudGin REST API) with thread-safe, de-duplicated work distribution, eliminating race conditions and raising throughput **70%**.
- **Performance:** Designed a custom **LRU cache** that removed **300,000+ redundant API calls** per cycle (batch runtime **10+ hours to 10–20 minutes**), and indexed slow queries to keep APIs under one second.

Trainee Software Engineer *Aug 2025 – Feb 2026*

- **Secure Backend-for-Frontend:** Owned, built and deployed on **AWS EC2** a citizen-facing 311 service portal; chose a BFF so the browser calls only the portal's own routes, removing cross-origin exposure and hiding internal ERP endpoints, parameters and architecture from the client.
- **Token & secret handling:** The server obtains and refreshes OAuth/bearer tokens and keeps API keys in server-side environment config; the browser holds only a session cookie.
- **Controlled file access:** Built an S3 photo-upload pipeline on short-lived **presigned URLs** with server-side processing, plus SNS/SES case alerts.

Software Engineer Intern – backend & integrations, converted to full time *Aug 2024 – Jul 2025*

Security Projects

Guardrails for an LLM Browser Agent (Personal) | *Python, Gemini API, Claude Code* 2026

- **URL risk vetting:** Built a pre-navigation checker that fetches a page without executing it, extracts deterministic signals (look-alike domains, redirect chains to unrelated hosts, credential forms) and has an LLM return a safe / caution / block verdict, cached per host for 7 days.
- **Prompt-injection defense:** Page text reaches the model only as quoted, untrusted data with JSON-only outputs; instruction-like text is flagged as suspicious and halts the agent instead of being followed.

JalDristi – Multi-Modal AI Analytics (Smart India Hackathon, team of 4) | *Python, Azure CV, OpenAI*

- Proposed the idea and built the AI module: Selenium social-media monitoring for crisis keywords, Azure Computer Vision captions fed into OpenAI summaries, and a Pandas criticality score that triages alerts.

Certifications & Training

Google Cybersecurity Professional Certificate
Microsoft Certified: AI Fundamentals (AI-900); Security, Compliance & Identity Fundamentals (SC-900)
PwC Acceleration Centers India – Cloud & Digital Launchpad (6-month training) | *DevOps, Cloud* 2024

Education

B.Tech in Computer Science Engineering, CGPA 8.5 – Siksha 'O' Anusandhan University 2021 – 2025