Dev Joshi

Chennai, Tamil Nadu, India | **Cloud Security & Software Engineer**

devvjoshi2005@gmail.com | linkedin.com/in/devjoshi2005 | github.com/devjoshi2005 | tryhackme.com/p/DJ1Hacks | https://leetcode.com/u/its_devj/

Professional Summary

Computer Science and Engineering undergraduate specializing in full-stack backend development, cloud security architecture, and applied AI compliance automation. Experienced in building high-throughput asynchronous services, multi-cloud IAM graph analyzers, and automated DevSecOps pipelines across AWS, GCP, and Azure. Strong algorithmic foundation with 997 LeetCode problems solved.

Education

Meenakshi Sundararajan Engineering College (Anna University) **2023 – 2027**
B.E. in Computer Science and Engineering | CGPA: 7.9/10.0 (up to Sem 6) *Chennai, India*

- **Core Coursework:** Data Structures & Algorithms, Operating Systems, Database Management Systems, Computer Networks, Object-Oriented Programming, Cryptography & Network Security, Introduction to Artificial Intelligence & Machine Learning

Sindhi Model Senior Secondary School **2022 – 2023**
Higher Secondary Education (Class XII) | Percentage: 83.3% *Chennai, India*

Sindhi Model Senior Secondary School **2020 – 2021**
Higher Secondary Education (Class X) | Percentage: 83% *Chennai, India*

Technical Experience & Job Simulations

Deloitte (Forage) **June 2025**
Cybersecurity & Log Analysis Simulation (Applied Experience) *Remote*

- Parsed and correlated web server and proxy access logs across 4 forwarding hops to isolate an anomalous credential-stuffing attack to a single malicious IP; documented incident timelines and defined 4 remediation controls (forced session revocation, token rotation, rate-limiting, and RBAC review).

Tata Consultancy Services (TCS Forage) **October 2026**
IAM Architecture & Identity Security Simulation (Applied Experience) *Remote*

- Designed an enterprise IAM migration strategy using Microsoft Entra ID (RBAC role hierarchies, Conditional Access policies, MFA enforcement, and automated lifecycle provisioning) for a simulated hybrid workforce.

Engineering & Security Projects

AuthMap – Cloud IAM Attack-Path Analyzer | Python, FastAPI, Neo4j, Node2Vec, scikit-learn, Next.js, TypeScript GitHub

- Built a FastAPI backend ingesting AWS and GCP IAM configurations into a Neo4j property graph (13 node types), executing Cypher traversals to detect 29 privilege-escalation patterns across a 1,000-principal account in 5s (30s end-to-end).
- Combined deterministic rule checks with Node2Vec graph embeddings & Local Outlier Factor (LOF) anomaly detection alongside a Next.js explorer (391 nodes in 1.5s), achieving 100% recall and 0 false positives across benchmark test sets.

Multi-Cloud GRC Compliance Engine | Python, LlamaIndex, ChromaDB, Prowler, AWS, Azure, Streamlit GitHub

- Built an automated compliance engine ingesting live AWS and Azure telemetry (Prowler, IAM, S3, CloudTrail) into a hybrid BM25 + vector RAG pipeline over 6 regulatory PDFs (350 pp, 4K chunks), maintaining 600 MB RSS on a t3.micro instance.
- Mapped live infrastructure telemetry to 232 controls across SOC 2, ISO 27001, and NIST CSF 2.0 with page-level citations at 200ms retrieval latency, reducing compliance triage time by 80% (30 -> 6 min/finding) and modeling financial risk exposure via FAIR (ALE = $180K/yr, INR 1.6 Cr).

DevSecOps Container Remediation Engine | Python, AWS Bedrock, AWS ECS, SonarQube, Trivy, ZAP, GitHub Actions GitHub

- Architected a 4-stage GitHub Actions CI/CD pipeline enforcing pre-deployment gates across SAST (SonarQube), SCA/container scanning (Trivy), DAST (OWASP ZAP), and Terraform IaC validation in 3.5 min per build.

– Integrated AWS Bedrock to parse normalized SARIF outputs and synthesize deterministic code and Dockerfile patch diffs in 2.3s per CVE; achieved an 83.3% (25/30) first-pass compile and regression pass rate on seeded container vulnerabilities in CI.

ResilienceOps – Cloud Native SOAR Engine | Python, Isolation Forest, Neo4j, AWS CloudTrail, OPA/Rego, Terraform GitHub

– Trained an unsupervised Isolation Forest pipeline over 30K real AWS CloudTrail log events across 7 behavioral features (13ms p95 inference latency) to detect lateral movement and credential-stuffing attacks at 54% recall (0.19 F1, 1.9% FPR).

– Mapped detected anomalies across a Neo4j property graph (142 principals -> 232 resources) to compute 4-hop blast-radius paths, gating automated Terraform containment behind OPA/Rego policy-as-code validation to reduce MTTD/MTTR to sub-35s.

Up – Event-Driven Alerting & Escalation Platform | Python, Django, Channels, Celery, Redis, PostgreSQL, React GitHub

– Engineered an alerting platform delivering notifications via WebSockets, email (Brevo), and SMS with HMAC-signed ack links and a SELECT FOR UPDATE SKIP LOCKED escalation sweeper.

– Load-tested with k6 on an EC2 t3.micro: sustained 30 events/s (560ms p95) and 500 concurrent WebSockets (1.0s p95 end-to-end delivery); guaranteed zero lost or duplicate messages across 1,300 chaos events using a transactional outbox and replayable DLQ.

ReconFlow – High-Throughput Payment Reconciliation | Java 21, Spring Boot, Spring Batch, PostgreSQL, AWS SQS, Next.js GitHub

– Built a 3-way financial reconciliation workbench utilizing Spring Batch checkpointing and PostgreSQL SKIP LOCKED, normalizing Razorpay, PhonePe, and bank CSV statements.

– Engineered an async ingestion pipeline (Next.js -> Spring Boot -> S3 -> SQS) processing 100K+ transaction rows at 850 rows/s on an EC2 t3.micro while sustaining 120ms p95 API query latency.

Google Cloud Security Environment | GCP (IAM, Cloud Armor, VPC Flow Logs, DLP API) GitHub

– Configured a Zero Trust reference architecture on GCP covering 5 security domains (IAM, VPC isolation, Cloud Armor WAF, storage encryption, and security monitoring).

– Built automated Cloud DLP pipelines to inspect, detect, and redact PII/PCI payload data before persistence, mapped directly to GDPR and DPDPA compliance frameworks.

Technical Skills

Languages: Python, Java (21), TypeScript, JavaScript (ES6+), SQL, Cypher, HTML5/CSS3, Bash

Applied AI & Graph ML: RAG Pipelines, LlamaIndex, ChromaDB, Hybrid Search (BM25 + Vector), Embeddings, OpenAI / LLM APIs, AWS Bedrock, Node2Vec, scikit-learn (Isolation Forest, LOF)

Backend & Async: Spring Boot, Spring Batch, Spring Security, FastAPI, Django REST Framework, Django Channels (ASGI/Daphne), Celery, WebSockets, RESTful APIs, OAuth2, JWT

Cloud Security & DevSecOps: AWS (IAM, GuardDuty, CloudTrail, S3, KMS, ECS, AWS Inspector, CloudWatch), Azure (Entra ID, Sentinel, NSGs, Log Analytics, Key Vault, VNets), GCP (IAM, Cloud Armor, Cloud DLP, VPC, Service Accounts), Docker (Container Security), Podman, Kubernetes Basics, Terraform (IaC), GitHub Actions (CI/CD), OPA/Rego, SonarQube, Trivy, OWASP ZAP, Prowler

Data Stores & Messaging: PostgreSQL (RDBMS, Indexing), Redis (Caching, Pub/Sub), Neo4j (Graph DB), SQLite, AWS SQS

Core CS & Security Concepts: Data Structures & Algorithms, Distributed Systems, Event-Driven Architecture, High Availability, Idempotency & Outbox Patterns, Threat Modeling, Zero-Trust Architecture | **LeetCode: 997 Solved** (118 Hard, 665 Medium)

Certifications & Credentials

Microsoft Certified: Azure Security Engineer Associate (AZ-500)

Microsoft Certified: Security, Compliance & Identity Fundamentals (SC-900)

Google / Coursera: Google Cloud Security Engineer Associate Specialization | Google Cybersecurity Professional

Amazon Web Services / Coursera: AWS Cloud Technical Essentials

IBM / Coursera: IBM Application Security & DevSecOps