

Vishisht Mishra

Gurugram, Haryana, India | +91-981-061-5840 | vishishtmishra150@gmail.com
vishisht.tech | github.com/Vishisht16 | linkedin.com/in/vishisht-mishra

SUMMARY

Final-year CSE student and independent security researcher whose disclosures have been logged by CERT-In, UK ICO and Singapore PDPC, with hands-on experience in Azure identity and access management and secure CI/CD.

EDUCATION

Central University of Haryana

B.Tech. in Computer Science and Engineering

Mahendragarh, HR

Aug. 2023 – July 2027

- **CGPA:** 8.11 / 10.0 (latest SGPA: 8.78) | **GATE 2026 Qualified:** score of 488 in CS/IT, earned in 3rd year

SECURITY RESEARCH & RESPONSIBLE DISCLOSURE

- **GirlScript Foundation:** Discovered and responsibly disclosed an exposure of 170,000+ individuals' data spanning 7 years and 57 countries, including PII of minors, emails and crypto wallet addresses, along with 16 production vulnerabilities (7 Critical, 5 High, 4 Medium). Logged by **CERT-In** (Ref: CERTIn-97826626), **UK ICO** (Ref: IC-531108-L5K5) and **Singapore PDPC** (Ref: 00667204).
- **Z.ai (Zhipu AI):** Reported **4 Critical and 8 High** severity vulnerabilities in the production systems of Z.ai, creator of the GLM models; acknowledged and under remediation.
- **Other Disclosures:** Reported additional vulnerabilities to global organizations via responsible disclosure, including one under review by Google.

EXPERIENCE

Azure Cloud Engineer

Luxury In Taste, Hosur

May 2025 – Nov. 2025

Remote

- Managed identity and access for the organization's Azure tenant as Entra Global Admin and Azure Contributor.
- Audited the cloud architecture and remediated inefficient resources, cutting Azure spend by 30–40%.
- Built and maintained GitOps CI/CD pipelines with GitHub Actions for the organization's repositories.

Research Intern, JNU – NMT model training on the Param RUDRA supercomputer

June 2026 – Aug. 2026

AI/ML Engineer, Tohund Guide Business Consultants – multi-tenant RAG platform

Feb. 2026 – Mar. 2026

Software Engineer, Fuzzy Nodes – sole engineer on a fleet & ERP platform, built end to end

Oct. 2025 – Jan. 2026

PROJECTS

HumaneProxy | Python, PyPI, MCP, FastAPI, SQLite, PostgreSQL, Redis

Apr. 2026 – Present

- Built and maintain an open-source AI safety middleware for LLM chat platforms, with a 3-stage classification pipeline that detects self-harm and criminal intent; 8.52K+ installs on PyPI.
- Trained a custom model; benchmarked the framework at 92% recall (SimpleSafetyTests) and 1.2% FPR (XSTest).
- Added an MCP server (bearer auth), swappable storage and a REST admin API with webhook alerts.

GKE Pipeline | GCP, Terraform, Docker, Prometheus, Grafana, Trivy, GitHub Actions, k6, Redis

Feb. 2026

- Built a GitHub Actions CI/CD pipeline with Trivy vulnerability scanning for zero-touch deploys to self-healing GKE infrastructure provisioned with Terraform.
- Validated resilience with k6 load tests, triggering HPA (2–10 pods) and cluster autoscaling (1–3 nodes).

TECHNICAL SKILLS & CERTIFICATIONS

Security: Vulnerability Discovery, Security Auditing, Responsible Disclosure, IAM (Microsoft Entra ID), Trivy

Cloud & DevOps: Microsoft Azure, GCP, Kubernetes, Terraform, Docker, GitHub Actions, Prometheus, Grafana

Languages & Frameworks: Python, TypeScript, SQL, FastAPI, Next.js, NextAuth, MongoDB, PostgreSQL

Certifications: GCP Associate Cloud Engineer, GitHub Actions, GitHub Foundations

ACHIEVEMENTS & LEADERSHIP

- **INR 2,00,000 in DoT Grants:** Awarded INR 1,00,000 twice (2025, 2026) by DoT, Govt. of India and TCIL as a 5G Innovation Hackathon national finalist; led “AI Subtitle Glasses”, an edge-AI wearable for the hearing impaired.
- **Lead, Google Developer Groups on Campus** (Aug. 2025 – Aug. 2026): led the university's developer community.