

# GAURAV KUMAR

☎ (+91)-8756746698 | ✉ gauravsingh12341@gmail.com | 🌐 Website | 📄 Github | 🔗 LinkedIn

## Education

MAY 2019	B. Tech. MECHANICAL ENGINEERING IIT Kanpur	7.6/10.0
APRIL 2015	Class XII (CBSE) SECONDARY DELHI PUBLIC SCHOOL,GAYA	94.8%

## Work Experience

**Lead Cloud Development Engineer at Citrix** July'25-Ongoing

- Added EDT support in the CGS tool to enable secure, low-latency communication over UDP for virtual apps and desktops.
- Enhanced Edge Service security by adding Web Application Firewall (WAF) and request rate-limiting controls.
- Extended EDT NAK statistics to include range support.

**Senior Software Engineer at Fortanix Inc.** June'19-June'25

- **ArmetAI Team**
  - \* Contributed to the design and development of a confidential Retrieval-Augmented Generation (RAG) pipeline.
  - \* Implemented core backend services and integrated all microservices.
  - \* Designed and implemented attestation mechanisms for a new AMD Confidential VM platform with GPU support, enhancing security and verification processes.
  - \* Architected and implemented security hardening for the Qdrant vector database.
  - \* Added protections against prompt injection, jailbreak attacks, toxicity, PII exposure, and hallucination in the RAG pipeline.
  - \* Packaged and configured Armet AI services for deployment in Customer-Managed VPCs.
- **Confidential Computing Manager (CCM) Team**
  - \* Conceived and implemented a confidential data clean room.
  - \* Spearheaded the Multi-Party Support feature, enabling collaborative workflow creation and execution across multiple accounts.
  - \* Developed a microservice for workflow monitoring, enabling efficient management of workflows.
  - \* Played a key role in the launch of the CCM SaaS product, a revolutionary platform for confidential computing (<https://ccm.fortanix.com>).
  - \* Architected and implemented core back-end functionalities, including the development of initial REST APIs, metering, and audit-logging microservices.
  - \* Delivered advanced features such as DCAP attestation support, multiple container registry configuration per account, Node Agent packaging, and an Operator for the CCM Node Agent.
  - \* Enabled DCAP attestation support during secure backend cluster join, enhancing trust verification in distributed environments.
  - \* Migrated CCM services to run on Ubuntu 24.04.
- **Data Security Manager**
  - \* Designed and developed a k8s plugin to encrypt secrets and ConfigMaps stored in etcd using DSM.
  - \* Implemented a plugin to securely inject secrets directly into Kubernetes workloads.

## Technical Skills

<b>Programming Skills:</b>	Rust: 5y, C++: 3y, Python: 2y, Go: 3y, C: 2y
<b>AI Skills:</b>	RAG, Prompt Engineering, Vector Databases, Embeddings, MCP
<b>Container Management:</b>	Docker, Kubernetes, OpenShift, Helm, Operator, Docker Compose
<b>Cloud:</b>	Azure, AWS, GCP, IBM Cloud
<b>Database:</b>	Cassandra, CockroachDB, Qdrant, Redis
<b>Debugging:</b>	gdb, strace
<b>Automation/Build:</b>	Jenkins
<b>Observability:</b>	Grafana, Splunk