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

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

- **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 tracking and management of workflows.
  - ∗ Contributed to integration with Azure Container Instances.
  - ∗ 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.
  - ∗ Integrated CCM with the IAM microservice.
  - ∗ Enabled DCAP attestation support during secure backend cluster join, enhancing trust verification in distributed environments.
  - ∗ Migrated CCM services to run o Ubuntu 24.04.
- **Data Security Manager**
  - ∗ Designed and developed a Kubernetes plugin to encrypt secrets and ConfigMaps stored in etcd using DSM.
  - ∗ Implemented a plugin to securely inject secrets directly into Kubernetes workloads.
- Actively involved in customer-facing issues, proof-of-concepts (POCs), mentoring, software engineering, and DevOps interviews.
- Collaborated closely with Frontend, QA and UX teams to ensure seamless integration and user experience.

Technical Skills

Programming Skills:	Rust: 5y, C++: 3y, Python: 2y Go: 3y, C: 2y,
AI Skills:	RAG, Prompt Engineering, Vector Databases, Tokenization, Embeddings
Container Management:	Docker, Kubernetes, OpenShift, Helm, Operator, Docker Compose
Cloud:	Azure, Aws, GCP, IBM Cloud
Database:	Cassandra, Cockroachdb, Qdrant
Debugging:	gdb, strace
Automation/Build:	Jenkins