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 and jailbreak attacks in the RAG pipeline.
- **Confidential Computing Manager (CCM) Team**
  - Contributed to the design and implementation of a confidential data clean room.
  - Designed and implemented the Multi-Party Support feature, enabling collaborative workflow creation and execution across multiple accounts.
  - Designed and developed a microservice for workflow monitoring, enabling efficient tracking and management of workflows.
  - Contributed to integration with Azure Container Instance.
  - Played a key role in launching the CCM SaaS product, a revolutionary platform for confidential computing (https://ccm.fortanix.com).
  - Architected and implemented core backend functionalities, including the development of initial REST APIs, metering and audit-logging microservices.
  - Developed advanced features such as DCAP attestation support, multiple container registry configuration per account, Node Agent packaging, and Operator for CCM Node Agent.
  - Integrated CCM with IAM microservice.
- **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.
- **Datashield Product Ownership**
  - Managed the Datashield product, an earlier version of CCM with on-premise deployment and limited functionalities
  - Oversaw all Datashield releases and led the integration of support for IKS versions 1.16, 1.18, and 1.19, Openshift versions 3 and 4, and Ubuntu 18.04.
- Actively engaged 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: 2y, C: 2y,
AI Skills:	RAG, Prompt Engineering, Vector Databases, Tokenization, Embeddings
Container Management:	Docker, Kubernetes, OpenShift, Helm, Operator, Docker Compose
Cloud:	Azure, Aws, IBM Cloud
Database:	Cassandra, Cockroachdb, Qdrant
Debugging:	gdb, strace
Automation/Build:	Jenkins