Muskan Kumari

Email | Portfolio | Twitter | LinkedIn | +91-9896876947

Academic Details

Year	Degree / Board	Institute	GPA / Marks(%)
2026	B.Tech in Mechanical Engineering	Indian Institute of Technology Delhi	7.18
2021	CBSE	S.R. Century School	96.6%
2019	HBSE	Sports Sainik Public School	9.40

Scholastic Achievements

- **ETH-Global Singapore Hackathon (2024):** Achieved First Position in the Rootstock track for the best project award.
- **ETH-Mumbai Hackathon (2024):** Won the main track in Zero Knowledge, Best project award out of 15,000 participants.
- **JEE Advanced Rank (2022):** Secured AIR 1147 (GE), AIR 8928 among 0.2 million candidates qualified for JEE Advanced.
- **JEE Mains Score (2022):** Achieved 98.3 percentile score among more than 1.1 million candidates in the JEE Mains.

Work Experience

Umbra Privacy | Backend Engineer **[December, 2025 – April, 2026]**

- Designed & implemented a **privacy-preserving cross-chain bridge** on NEAR Intents, used HKDF-derived ephemeral keypairs to ensure source & destination transactions remain unlinkable on-chain, eliminating visible cross-chain graphs.
- Built a production-grade Solana data indexer in Rust with Diesel ORM, handling complete historical backfills and real-time ingestion from RPC streams. Delivered consistent, queryable historical state for private transaction history for user dashboard.
- Developed a **Solana Gasless Relayer** as RESTful relayer service allowing users to pay fees in SPL tokens via Jupiter pricing integration. Implemented Redis-backed rate limiting and automated fee-payer signing.
- Led the implementation of a **Groth16 Phase-2 trusted setup** system in Rust using **snarkjs**, including a Postgres-backed coordinator, Redis HMAC-signed job queue, WebSocket APIs & concurrent workers for **powers-of-tau, R1CS**, zkey processing.
- Built a dual-mode participant CLI (TUI + headless) supporting parallel **multi-circuit contributions**, with S3 artifact storage, timeout watchdogs, dead-letter queues, and API rate limiting for reliable large-scale ceremony orchestration.

Encifher | Cryptography Research Engineer **[March, 2025 – Dec, 2025]**

- Designed & implemented end-to-end a **Rust-based Key Management System (KMS)** using threshold ElGamal encryption.
- Implemented relaxed discrete log DKG and **Pedersen Verifiable Secret Sharing**, enhancing trustless key management protocols.
- Implemented a **Bulletproof protocol** tailored for the Solana chain, enabling efficient zero-knowledge range proofs.
- Worked with **elliptic curve accumulators** to build privacy-preserving integrity checks, ensuring verifiable state consistency.
- Conducted end-to-end **STRIDE threat modeling** for Encifher systems by mapping trust boundaries and data flows, identifying spoofing, tampering, repudiation, information disclosure, DoS, and privilege-escalation risks, and defining mitigations to strengthen KMS and cryptographic infrastructure.

Projects

BrainfuckVM | ETH-India 2024 **[Nov, 2024 – Dec, 2024]**

- Designed and implemented Prover and Verifier for **Brainstark Zero-Knowledge Virtual Machine** completely in Rust.
- Engineered foundational **ZKVM** libraries, including custom implementation of Fast Reed-Solomon Interactive Oracle Proofs.
- Built supporting crates from scratch, showcasing strong expertise in secure systems programming & cryptographic protocol.

Zk-Market | ETH-Global Singapore 2024 **[Sep, 2024 – Oct, 2024]**

- Built Zk-Market, a groundbreaking marketplace bridging Web2 and Web3 ecosystems using zero-knowledge proofs.
- Leveraged **ZK-TLS** to establish secure connections with Web3 networks, ensuring privacy and trustless verification.
- Enabled efficient on-chain verification of Web2 data using proxy-based ZK-TLS integrated with Reclaim Protocol.

Zero-knowledge compiler | ETH-Mumbai Hackathon 2024 **[March, 2024 – April, 2024]**

- Used the research paper **CirC: Compiler infrastructure for proof systems, software verification, and more**
- Developed a versatile and efficient compiler for generating and verifying proofs of high-level language computations.
- Implemented support for C, Rust, Python, Solidity, and Zokrates, compiling to **Rank One Constraint System (Groth16)**.

Quark Layer | BlocSoc R&D **[April, 2024 – March, 2024]**

- Decentralised proof verification and aggregation layer built for verifying zero-knowledge proofs.
- Provides near-instant soft crypto-economic guarantees and delayed cryptographic guarantees on proof verification result.
- Supports Succinctlabs sp1, Risczero's zkvm, 0xpolygonmiden, Jolt, enabling interoperability & flexible deployment.

Veritas | **AI-Powered Third-Party-Risk-Assessment** **[April, 2026 – Present]**

- Built and deployed on Vercel a Next.js 16 (App Router) app that streams Zod-validated structured output from Claude via the Vercel AI SDK v6 to power a real-time third-party security-assessment UI.
- Built a structured data pipeline to ingest multi-format vendor files server-side, progressively mapping text to 15 NIST CSF 2.0 controls, CWE metrics, and decoupled framework abstractions (ISO 27001/PCI DSS).

Technical Skills

- **Programming Languages & Tools:** Java, Python, Solidity, Rust, SQL, R, Typescript, Node.js, Docker, Stride.
- **Libraries:** TensorFlow, PyTorch, Scikit-learn, Pandas, NumPy, Circom, Matplotlib, Graphviz, XGBoost, Diesel.
- **Web3 Development & Frameworks:** Ethereum Virtual Machine, Hardhat, Ethers, Web3.js, Foundry (Solidity), Anchor
- **Zero Knowledge:** Hands-on experience with Groth16 protocol, Halo2, Plonk and sum check protocol, zkvms
- Hands-on with core concepts & infrastructure of Web3: EIPs, NFT & ERC20 Token standards, DApps
- Hands-on experience with FRI (Fast Reed-Solomon Interactive Oracle Proofs of Proximity) protocol in Rust

Certifications

- **ACM Cryptography Summer School, IIT Bombay:** Certified participant covering ZK proofs, MPC, FHE, & blockchain.
- **OWASP API Security Top 10,** APIsec University: Deep-dive into the 2023 OWASP API Security Top 10.
- **Supervised Machine Learning: Regression and Classification,** DeepLearning.AI & Stanford University
- **Advanced Learning Algorithms,** DeepLearning.AI & Stanford University

Positions of Responsibility

- **Overall Coordinator, BlockChain Society, IIT Delhi:** Led a team of 50+ members & collaborations with industry experts. [April, 2025 - May, 2026]
- **Coordinator, BlockChain Society, IIT Delhi:** Led research initiatives & organized workshops on defi, distributed systems [April, 2024 – March, 2024]
- **Executive, BlockChain Society, IIT Delhi:** Organized and led workshops on blockchain fundamentals, cryptography, Dapps [June, 2023 – May, 2024]
- **Football – Vice Captain, Himadri, BHM:** Led squad in inter-hostel tournaments & fostered team spirit as part of the BHM [June, 2023 – May, 2024]