



ARINDAM SAL



ACADEMIC DETAILS

| Year | Degree / Board | Institute | GPA / Marks(%) |
|------|--|--------------------------------------|----------------|
| --- | M.Tech in Cyber Security | Indian Institute of Technology Delhi | 7.38 |
| 2024 | B.Tech in Computer Science and Engineering | MCKV Institute of Engineering | 9.59 |
| 2020 | West Bengal Council of Higher Secondary Education (12th) | Santragachi Kedarnath Institution | 83.6% |
| 2018 | West Bengal Board of Secondary Education(10th) | Tatarpur High School | 92.71% |

IIT DELHI THESIS

Title: Secure Boot and Trusted Logging for Automotive ECUs with HSM & TEE

Supervisor: Prof. Kolin Paul, Department of Computer Science and Engineering

Description: Building automotive microcontroller security stack to protect **ECUs** against firmware tampering, unauthorized modifications, and software attacks; Implementing **secure boot, trusted logging, and authenticated updates**, scaling from **Raspberry Pi** prototype to **Infineon AURIX™ TC375** with **HSM-backed** key storage and **TEE**-protected runtime.

- Implemented multi-stage validation (**Bootloader → U-Boot → Monitor**), ensuring only signed firmware executes.
- Prototyped secure boot on **Raspberry Pi**, achieving **100%** authenticated execution with **<5%** verification overhead.

PROJECTS

IIT Delhi Course Projects

- **Identity-Based Cloud Integrity Auditing With Data Hiding (Prof. Huzur Saran)** (March, 2025 - June, 2025) :
 - Developed **identity-based cloud integrity auditing** with sensitive data sanitization, achieving **70% peak** and **45% average speedup** through optimized privacy-preserving algorithms.
 - Implemented **parallel verification** with tamper-evident logging and multi-layered blinding, enabling **O(1)** audit scalability, **58% faster** processing, and strong resistance to tampering and privacy attacks.
- **Secure Communication & Web Application Security Testing (Prof. Huzur Saran)** (March, 2025 - April, 2025) :
 - Built a TLS client in Python (**ssl, socket**) implementing handshake, CA/hostname verification, and secure **HTTP communication**; validated via **Wireshark**.
 - Performed web vulnerability assessments using **Burp Suite and Nmap/NSE**, identifying **XSS, TLS/SSL misconfigurations, CVE-mapped services**, and recommending mitigations per **OWASP** guidelines.
- **Android Application Security Testing (Prof. Rajesh Pal)** (March, 2025 - May, 2025) :
 - Performed a security audit of a vulnerable Android banking app, identifying and exploiting flaws including insecure broadcast receivers, exported activities, weak cryptography (**hardcoded AES keys**), insecure logging, and plaintext HTTP transmission.
 - Used **Frida, Apktool, Burp Suite, Genymotion emulator, and ADB** to patch APKs, **bypass root detection, intercept network traffic, and manipulate parameters**; proposed mitigations aligned with Android security best practices.
- **Cryptographic Secure Messaging System using AES (Prof. A.K. Bhatia)** (July, 2024 - September, 2024) :
 - Built an **end-to-end encrypted client-server messaging system** using **AES-CBC** with **PBKDF2 key derivation**, ensuring confidentiality, integrity, replay attack prevention (**via unique IVs**), and encrypted username privacy
 - Implemented **secure storage and administration features** with **SQLite-backed encrypted message logging**, master-password protected server controls, and **multi-client support**, providing a robust foundation for real-world secure communication

TECHNICAL SKILLS

- **Programming Languages:** C (Proficient), C++ (Proficient with STL), Python (Core), SQL
- **Software & Tools:** Git, MySQL, LINUX, Wireshark, Burp Suite, Android Debug Bridge, NMap, Jadx-Gui

SCHOLASTIC ACHIEVEMENTS

- Received Outstanding Teaching Assistant Award in COL100(Introduction to Computer Science), 2024-2025
- Qualified GATE 2024 CS/IT

POSITIONS OF RESPONSIBILITY

- **Teaching Assistant for the course** Introduction to Computer Science(COL100)-**Best TA Award** & Data Structures and Algorithms(COL106), IIT Delhi (Jul, 2024 - Present)



ARINDAM SAL



IIT COURSE

| Degree | Institute | CGPA | Dept. Rank |
|--------------------------|--------------------------------------|------|------------|
| M.Tech in Cyber Security | Indian Institute of Technology Delhi | 7.38 | --- |

COURSES DONE

Advanced Data Structures, Computer Networks, Cryptography & Computer Sec., Introduction To Blockchains, Cryptocurrencies, And Smart Contracts, Resource Management In Computer Systems, Minor Project, Networks & System Security, Special Topics In Cyber Security