



# Souvik Mukherjee

Computer Science & Engineering

231110405

Indian Institute of Technology Kanpur

Languages: English, Hindi, Bengali

✉ souvikm23@iitk.ac.in ☎ +91-8158920720 🌐 souvikcseiiitk 🌐 Souvik Mukherjee 📁 Portfolio

| Education       | University/School          | Subject/Discipline        | Year    | GPI/% |
|-----------------|----------------------------|---------------------------|---------|-------|
| Post Graduation | IIT, Kanpur                | MS-R, CSE (Cybersecurity) | 2023-25 | 9.80  |
| Graduation      | VIT, Vellore               | Major, ME and Minor, CSE  | 2017-21 | 9.16  |
| Intermediate/+2 | Sri Chaitanya, Vizag (HSC) | STEM                      | 2015-17 | 92.00 |
| Matriculation   | Sri Chaitanya, Vizag (SSC) | STEM                      | 2015    | 10.00 |

## RESEARCH EXPERIENCE

- **Face Morphing Attack Generation and Detection (Digital Forensics) (M.S-R Thesis);**  
Guide: Prof. Nisheeth Srivastava  
Impact: 10L+ students/year (Nov'23 - Present)
  - **Face Morphing:** A digital image manipulation technique that seamlessly blends two facial images, creating a fake blended face of two subjects.
  - **Misuse:** A deceptive tool in exams, where a morphed image combines the faces of a bright and a dull student, allowing the latter to pay the former to take exams on their behalf, thus gaining admission.
  - **Types:** Majorly two types of morphs, Landmark based and Deep-Neural-Network based (GAN/style-GAN). Done on two format's of images, JPG and PNG.
  - **Progress made:** We have achieved close to 99% accuracy for PNG's and around 60% for JPEG's, using Error Level Analysis (ELA) and contours in image processing. We're still working on JPEG's to improve accuracy.

## PROJECTS

- **DOM and DFA Attack on AES (CS666: H/W Security for IoT)(A Grade)** Guide: Prof. Urbi Chatterjee 🌐 (July'23-Nov'23)
  - **For the DOM/DPA analysis, Objective:** Recovering AES secret key bytes using Differential Power Analysis (DPA).
  - **Technique Used:** Implemented Difference of Mean Attack with zero and one bin arrays and successfully retrieved asked key bytes from power traces.
  - **In DFA analysis:** We conducted the **fault injection** and **formed equations** to iteratively retrieve the key of said bytes.
- **Packet Capture Analysis (CS628: CSS)(A Grade)** Guide: Prof. Angshuman Karmakar 🌐 (July'23-Nov'23)
  - **Objective:** Analyzed .PCAP files for SQL injection and XSS attacks using Wireshark.
  - **Methodology:**
    - \* Filtered HTTP packets to identify potential SQL injection commands like UNION SELECT.
    - \* Detected session ID theft via cookies and MD5 hashed password theft.
  - **Insights:**
    - \* Recognized vulnerabilities in MD5 hashed passwords, susceptible to rainbow table attacks.
    - \* Implemented safety measures against XSS and SQL injection attacks.
  - **Skills:** Security analysis, Wireshark, vulnerability mitigation.
- **Designing efficient NTT, PWM & I-NTT (CS674 PQS) (A Grade)** Guide: Prof. Debapriya B. Roy 🌐 (July'23-Nov'23)
  - Firstly, we're given 2 functions, we computed the **Fourier transform** for each one of them (using the **Cooley-Tukey NTT algorithm**). Secondly, we performed **point wise multiplication** to the transformed functions.
  - Lastly, we did **inverse NTT** on the last output. (Using the **Gentleman-Sande inverse INTT algorithm**)
- **Breaking Companion Arbiter PUF (CAR-PUF) using ML (CS771)** Guide: Prof. Purushottam Kar 🌐 (Jan'24 - Apr'24)
  - A CAR-PUF employs two arbiter PUFs, along with a secret threshold value  $\tau$ . Given same challenge to both, the absolute difference in timings is calculated. If  $|\Delta w - \Delta r|$ , is less than or equal to  $\tau$ , the response is 0; otherwise, it's 1.
  - Derived a detailed mathematical derivation demonstrating how a CAR-PUF can be compromised by a single linear model.
  - Wrote a code to solve this problem by learning the linear model  $W, b$  using the training data. Model used was '**model = LogisticRegression(C=1.0)**'. We mapped input features from 32 dimensions to 528, to get a proper linear fit. We had also computed how various hyper-parameters affected training time and test accuracy.
- **Escaping the Caves(CS641)(Modern Cryptology) (A Grade)** Guide: Prof. Manindra Agrawal 🌐 (Jan'24 - Apr'24)
  - Methodically **Analyzed and Decoded** a range of cryptosystems namely, **Substitution cipher, PlayFair cipher, EAEAE, DES**.
  - Utilized advanced techniques to exploit cryptosystems, methods such as **frequency analysis, differential cryptanalysis**.
- **Project GATE CSE GPT (Winter LLM Bootcamp, Pathway x IIT-K x IIT-BHU, Non-Academic) 🌐** (Feb'24)  
Impact: 1L+ students/year
  - A chatbot-GPT powered by **OpenAI & Pathway**. Aims in helping students with interview, PYQ, test-series, the main exam and other common doubts, related to GATE CSE exam, specifically who are facing difficulty in affording coaching, with the help of Pathway's LLM App, and a **Dropbox** at backend
  - The LLM App enables AI-powered search from multiple unstructured documents like prev. interview experiences, PYQ's, topper's notes, etc and indexes input data in real-time just after you upload files to the cloud storage.

## RELEVANT COURSES AND TECHNICAL SKILLS

---

- **Mtech Courses** : CS771 Introduction to Machine Learning, CS641 Modern Cryptology, CS628 Computer Systems Security, CS666 Hardware Security for IOT Devices, CS674 Post Quantum Security
- **Btech Courses** : CSE2003 Data Structures & Algorithms, CSE2004 Database Management System, CSE2001 Computer Architecture, ONL1021 Essentials of Machine Learning and Organization, CSE1003 Digital Logic and Design
- **Programming/Scripting Languages**: C, C++, Python, Java, JavaScript, Verilog HDL, HTML, CSS, MySQL.
- **ML Libraries/Utilities/Tools**: Scikit-learn, Tensorflow, PyTorch, NumPy, OpenCV, Pillow, Pandas, Matplotlib, Git,  $\LaTeX$ , Google Colab, Jupyter.

## POSITIONS OF RESPONSIBILITY/EXPERIENCE

---

- **Head TA**, for the second semester in the **ESC111/112, Fundamentals of Computing**, which included, management of examinations and duties of other TA's, apart from the basic doubt resolving. (Jan'24-May'24)
- **Teaching Assistant** : Two semesters of assisting **ESC111/112, Fundamentals of Computing** students with doubt resolution, lab test management and grading assignments (Aug'23-May'24)
- **Graduate Engineer Trainee (GET) & Associate Engineer at L&T Technology Services** 🌀🌀 (Aug'21-March'22)

## ACADEMIC ACHIEVEMENTS AND RECOGNITION'S

---

- Awarded with the **Academic Excellence Award** for the semester '2023-24 First' for ranking among the **top 10%** of scorers in the department. 🌀🌀
- My project was recognized among the **top 3** open-source projects in the Winter LLM Bootcamp cohort, offered by **Pathway X P-Club IIT Kanpur x CoPS IIT BHU** 🌀
- **First Position** among 689 registered participants in the 'Altair Data Science Contest' conducted by Altair x Techkriti'2024 🌀
- Selected for **ACM India Summer Schools 2024**, held at **IIT Bombay**, offered by Trust Lab, IIT Bombay. 🌀🌀  
Only **60 students were shortlisted from all over India out of 550 applied**, based on profile shortlisting.  
**Name of the school offered**: Theoretical Foundations of Cryptography  
**Topics Covered**: Information theory, secret sharing, randomness extractors, computational tools, symmetric-key and public-key encryption, signatures, Zero-Knowledge proofs, Cryptography for Blockchains, and Secure Multi-party Computation.  
**Speakers**: From Microsoft Research India, IBM Research India, IIT Bombay, IISc (June 3 to 13, 2024)

## CERTIFICATIONS

---

- Supervised Machine Learning: Regression and Classification, by **deeplearning.AI & Stanford** 🌀
- Advanced Learning Algorithms, by **deeplearning.AI & Stanford** 🌀
- Machine Learning Professional Certification, by **RAPIDMINER, Altair** 🌀
- The Return Journey Hackathon, by **IIT Kanpur x Google Developer Student Clubs - Certificate Of Achievement** 🌀
- The joy of computing using Python, by **NPTEL, IIT Madras** 🌀
- Introduction to Generative AI, by **Google Cloud Skills** 🌀
- Data Analytics Methods for Marketing by **Meta** 🌀
- Participated in the **ISRO- Outreach Programme**: and completed the following courses:
  - Basics of Remote Sensing Geographical Information System and Global Navigation Satellite System 🌀
  - Overview of Web GIS Technology 🌀
  - Earth Observation for Carbon Cycle Studies 🌀
- Attended the workshop on Data and AI with Microsoft Azure held On Campus (on 10 April 2024, at L7 (LHC))

## EXTRA-CURRICULARS

---

- Part Of **American Society of Mechanical Engineers (ASME) college chapter, VIT Vellore** . 🌀 (Dec'17-Dec'19)  
I have made significant contributions in roles such as coordinator, events management, and primarily as a member of the design team. My skills encompass proficiency in Photoshop and Premiere Pro.
- **2018, Crew member, Mechnovate 2018**, an event by **ASME India, VIT Vellore** 🌀
- **2019, Coordinator, International Conference on Materials, Manufacturing and Modelling (ICMMM) 2019**, organized by the School of Mechanical Engineering (SMEC), VIT in association with ASME Chapter, VIT 🌀
- **2019, Manager, E-Fest Asia Pacific 2019**, an event by **ASME, USA** 🌀🌀

## NATIONAL LEVEL EXAMS TAKEN

---

- **Graduate Aptitude Test in Engineering, GATE in CSE, All India Rank: 507, Score: 690, Percentile: 99.33**
  - Fundamental of computer science and engineering, Data Structure and Algorithms, Database, Computer Architecture, Computer Networks, Operating Systems, Compiler Design, Theory Of Computation, Digital Logic and Design, Discrete & Engineering Math. 🌀**Scorecard**