Souvik Mukherjee

Computer Science & Engineering 231110405

Indian Institute of Technology Kanpur Languages: English, Hindi, Bengali

souvikm23@iitk.ac.in +91-8158920720 souvikcseiitk Souvik Mukherjee Portfolio

Education	University/School	Subject/Discipline	Year	CPI/%
Post Graduation	IIT, Kanpur	MS-R, CSE (Cybersecurity)	2023-25	10.0 (**)
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	10.0

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 τ. Given same challenge to both, the absolute difference in timings is calculated. If $|\Delta w - \Delta r|$, is less than or equal to τ, 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) 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 :** Introduction to ML, Modern Cryptology, Computer Systems Security, Hardware Security for IOT Devices, Post Quantum Security
- **Btech Courses :** Data Structures & Algorithms, Database Management System, Computer Architecture and Organization, 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

- **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*)
- I was the **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*)

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**
- Selected for **ACM India Summer Schools 2024**, to be held at **IIT Bombay**, offered by Trust Lab, IIT Bombay.
  Only **40 students are shortlisted from all over India**, based on profile shortlisting.
  Name of the school offered: Theoretical Foundations of Cryptography (*To be held from June 3 to 13, 2024*
- Attended the workshop on Data and AI with Microsoft Azure held On Campus (on 10 April 2024, at L7 (LHC))