Vishal Kumar

Department of Computer Science & Engineering
Indian Institute of Technology, Kanpur
vishalku23@iitk.ac.in / +91-9024945939
vishalsavarna / vishalsavarna

Education

Year	Degree/Certificate	Institute	CPI/%
2023-Present	M.Tech/CSE(CyberSecurity)	Indian Institute of Technology, Kanpur	8.83/10
2019-2023	B.Tech/Computer Science & Engg.	Institute of Engineering and Management, Kolkata	8.66/10
2018	Central Board of Secondary Education(CBSE)	Holy Mission Sr. Sec. School, Dighra	75.00%
2016	Central Board of Secondary Education(CBSE)	Holy Mission Sr. Sec. School, Dighra	9.8/10

Research Experience

- **Combating DeepFakes with GAN-Based Watermarking** (M.Tech Thesis) Guide: Prof. Soumya Dutta (*Apr'24 - Present*)
  - Developed a DeepFake detection method using GAN-based **visible** watermarking with **reconstructive regularization**.
  - Evaluated watermark robustness across GANs and datasets, preserving image quality with minimal **SSIM** and **FID** impact.
  - Studied how **Fine-Tuning**, **Cropping** and **Post-processing** impact watermarked DeepFake detection and resilience.
  - Optimized GAN loss via **Ablation studies** to balance watermark quality and detection performance.
  - Future work will aim to improve robustness against adversarial attacks and explore **dual watermarking** techniques.

Course Projects

- **CyberFortify** | CS628: Computer Systems Security | Prof. Angshuman Karmakar (*Aug'23-Nov'23*)
  - **Least Privilege Enforcement:** Refactored C code to limit root access, enhancing system security.
  - **Vulnerability Analysis:** Identified and mitigated buffer overflow and format string vulnerabilities.
  - **Web Exploits:** Performed SQL injection, XSS, and CSRF attacks on a vulnerable web server.
  - **Packet Analysis:** Analyzed PCAP files with Wireshark to uncover insights from SQL injection and XSS attacks.
- **ShieldSecure IoT** | CS666: Hardware Security for IOT | Prof. Urbi Chatterjee (*Aug'23-Nov'23*)
  - Designed **Verilog modules** for hardware security, including 8-bit full adders, 4-bit multipliers, and Johnson counters.
  - Implemented an iterative **AES-128** encryption architecture, optimizing key expansion and encryption in hardware.
  - Conducted **side-channel analysis** on AES encryption, including **differential fault** and Mean Attacks for key extraction.
  - Evaluated 64-bit **Arbiter-PUFs** on FPGA devices, calculating uniqueness, reliability, and uniformity using **10K CRPs**.
- **Escaping the Caves** | CS641: Modern Cryptology | Prof. Manindra Agrawal (*Jan'24-Apr'24*)
  - Methodically **Decoded** a range of cryptosystems namely, **Substitution cipher, Playfair cipher, DES, EAEAE**.
  - Applied advanced techniques to exploit cryptosystems, methods such as **frequency analysis, differential cryptanalysis**.
- **Linear Model Analysis for CAR PUFs** | CS771: Intro to ML | Prof. Purushottam Kar (*Jan'24-Apr'24*)
  - Harnessing dual arbiter PUFs and a concealed threshold τ, the CAR-PUF outputs 0 when $|\Delta w - \Delta r| \leq \tau$; else 1.
  - Constructed a novel approach for CAR-PUF modeling with linear models, expanding features from **32** to **528** dimensions.
  - Achieved a prediction accuracy of over 98% for CAR-PUF responses using **ML** techniques (LinearSVC, LogisticRegression).
  - Examined the impact of **hyperparameters (C, loss, tol)** on training time and accuracy, offering optimization insights.

Self Projects

- **BalBuddhiVidya:** Ancient wisdom for modern minds (*Jun'24-Present*)
  - Crafted a comprehensive yoga and fitness platform with **dedicated dashboards** for users, instructors, and admins.
  - Integrated **AI chatbots** to provide instant fitness advice, tips, and support, driving a 25% increase in user interaction.
  - Built **data visualization** tools for tracking fitness progress through interactive charts and graphs.
  - Implemented **social features** for users to connect, join groups, share progress, and participate in challenges.
  - Pioneered **AR** workout modules, creating immersive fitness experiences with virtual trails and 3D yoga instructors.
- **SmartSignCalc:** Bridging Gesture & Arithmetic (*Jun'24-Present*)
  - Engineered a real-time hand sign recognition system with **CNNs**, achieving **99.90%** accuracy on test data.
  - Created a custom dataset with webcam-captured hand gestures, applying **Gaussian blur** and **Adaptive thresholding**.
  - Built a CNN model in **TensorFlow** to convert hand signs into **Math expressions**.
  - Enhanced accessibility for **users with disabilities** by utilizing hand sign recognition as an intuitive input method.

Relevant Courses and Technical Skills

- **MTech Courses:** Introduction to ML, Modern Cryptology, Computer Systems Security, Hardware Security for IOT Devices.
- **BTech Courses:** Data Structures & Algorithms, Operating Systems, Computer Networks, Database Management System.
- **Programming/Scripting Languages:** C, Java, Python, JavaScript, HTML, CSS, SQL, Verilog HDL.
- **Libraries/Tools:** PyTorch, React, TensorFlow, Scikit-learn, NumPy, Pandas, Matplotlib, Git, LaTeX, Google Colab, Jupyter.

Academic Achievements & Positions of Responsibility

- **GATE CS:** Secured All India Rank 530 in GATE CS 2023 (*Jun '23*)
- **Student Guide**, Institute Counselling Services, IIT Kanpur: Mentoring freshmen, giving academic support. (*Jul'24-Present*)
- **Teaching Assistant(CS677):** Assisted with course instruction, grading, and student support. (*Jul'24-Nov'24*)
- **Teaching Assistant(ESC111/112):** Assisted with doubt resolution for students across two semesters. (*Aug'23-Apr'24*)