SOMESH VAS AERUPULA

Department of Computer Science & Engineering
Indian Institute of Technology, Kanpur

✉ someshva22@iitk.ac.in / ☎ +91-9963935394
Somesh Vas / Somesh Vas

Education

Year	Degree/Certificate	Institute	CPI/%
2022-Present	M.Tech/CyberSec.	Indian Institute of Technology, Kanpur	7.17/10
2016-2020	B.Tech/Computer Science & Engg.	TKREC,Hyderabad	7.49/10
2014-2016	CBSE(XII)	Kendriya Vidyalay Hyderabad	75%
2013-2014	CBSE(X)	Kendriya Vidyalay Hyderabad	10/10

Work Experience

- **TCS |** (System Engineer) *(Apr'21 - July'22)*
  - Successfully integrated Linux distribution (operating system based on Linux Kernel) **SUSE Linux Enterprise** Services on top of Regional Processor Virtual Machines
  - Designed features for **automatic streamlining of logs** to external remote server through the host node and improving the accuracy of Global Positioning Systems (GPS) via **Chronyd** feature.
  - Performed Upgrade Procedures, LDAP (Lightweight Directory Access Protocol) configurations, Network Transfer Protocol (NTP) server configuration, Central Processing and Regional Processing configurations, Maiden installations and Stack Deployment using OpenStack on virtual nodes.
  - Worked on Quick Studies and One-Pager related to CIS-CAT assessments, PNF (Physical Network Function) to VNF (Virtual Network Function) Lightweight restoration in **VMWare** and **Rsyslog (Remote Syslog)** feature.

Research Experience

- **Efficient Code-Based Scheme for Post-Quantum Era**(M.Tech Thesis) *(May'23 - Present)*
  Guides: Prof. Angshuman Karmakar
  - Investigating efficiency of **NIST Round 4 code-based** cryptographic scheme submissions.
  - Developing high-performance GPU-accelerated library for optimized Key Encapsulation Mechanism (KEM).
  - Utilized **CUDA Toolkit** to **parallelize matrix and polynomial operations**, significantly enhancing performance.
  - Findings potentially impact real-world deployment of Signature schemes and NIST's Post-Quantum Cryptography standardization.
  - **Research Areas :**Post- Quantum Cryptography

Course Projects

- **Publisher-Subscriber scheme for Ethereum Smart Contracts** (CS731) Guide: Prof. Angshuman Karmakar (Jan'23 - May'23)
  - Implemented a publisher-subscriber model resembling **Ethereum's functionality**, ensuring users anonymity preferences
  - **Tested** with 400+ publishers and subscribers, showcasing seamless real-time operation, ensuring the project is versatile.
  - **Implemented smart contracts** to perform diverse functions of both publishers and subscribers within the project.
  - Utilized **MongoDB** for efficient data storage, backend **NodeJS** and frontend **ReactJS** for an improved user experience.
  - Enhanced efficiency by implementing a Virtual Event Queue in Kafka for asynchronous data movement.
- **Detection and Prevention of DDoS attacks in VANETs** (CS668A) Guide: Prof. Sandeep Kumar Shukla (Sep'22 - Oct'22)
  - Implemented **DDoS detection and prevention** system for VANET networks.
  - Conducted practical testing in a network setup using MiniNet and POX.
  - Implemented over individual nodes for self reliance and preventing resource exhaustion.
  - Trained a **ML model** to identify DDoS traffic which provided an accuracy around 96
  - **Integrated with deterministic algorithm** for better efficiency and speed.
- **Differential Fault Attack on AES - Analysis and Exploitation** (CS666A) Guide: Prof. Urbi Chatterjee (Sep'22 - Nov'22)
  - Executed a Differential Fault Attack on AES, uncovering byte-level discrepancies in real-time ciphertext pairs.
  - Employed equations involving S-box and ciphertext variations to pinpoint the fault location.
  - Successfully demonstrated the potential vulnerability of AES to differential fault attacks.
- **Escaping the Caves using Cryptographic Algorithms** (CS641A) Guide: Prof. Manindra Agrawal (Jan'23 - Apr'23)
  - **Analyzed and Decoded** various cryptosystems namely, **Substitution cipher, PlayFair cipher, EAEAE, DES, RSA, Hashing**
  - Exploited cryptosystems using techniques like **frequency analysis, differential cryptanalysis**.
- **AES cracking through Mutual Information Analysis** (CS669A) Guide: Prof. Debapriya Basu Roy (Jan'23 - Apr'23)
  - Cracked AES key using Mutual Information Analysis through power traces obtained from real time AES encryption
  - Analyzed trace data from an FPGA-based AES implementation to recover the 128-bit AES Key using mutual information analysis.
  - Designed a custom leakage model, focusing on the 9th round AES S-Box output, to enhance key recovery accuracy
  - Applied mutual information techniques to extract key information from noisy traces, highlighting expertise in cryptography and signal processing.
  - Demonstrated successful AES key recovery by adapting mutual information analysis to real-world trace data, showcasing advanced problem-solving skills.
- **Computer Systems Security Lab** (CS628A) Guide: Prof. Sandeep Kumar Shukla (Jan'23 - Apr'23)
  - Learned to use NMAP, Wireshark and other tools for packet sniffing.
  - Learned to analyse nearby packet traffic through various labs of Web Security and Network Security.
  - Had hands on session in exploiting Application Security.

OTHER PROJECT

- **Developed website for Cell for Differently abled persons (**CDAP IITK**)** (June’23-Jul’23)
  - Designed and developed the official website for CDAP IITK.
  - Successfully launched the live website accessible at: http://www.iitk.ac.in/pwd/.
- **DCaptcha Solver** (Self Project) (June’23-Jul’23)
  - Trained a simple fast ML model to break captcha.
  - Works over hex characters with an accuracy over 99.
- **CSRNet Implementation for Congested Scene Recognition** (Self Project) (Jan’23 - Apr’23)
  - Implemented the CSRNet paper to develop a model for accurate crowd count estimation and density maps using the ShanghaiTech dataset.
  - Employed a two-component architecture comprising a 2D feature extraction CNN and a dilated CNN for broader reception fields.
  - Demonstrated exceptional model performance on the ShanghaiTech dataset, achieving a 47.3.
  - Extended model applications to counting various objects within congested scenes.

TECHNICAL SKILLS

- **Programming Languages**: C, C++, Python, MySQL
- **Web Development**: HTML, CSS, JavaScript, React JS, Node JS
- **Blockchain:** Ethereum Solidity
- **Smart Contracts:** Ethereum Smart Contracts, Event Handling
- **GPU Programming:** CUDA
- **Version Control**: Git, GitHub
- **Containerization:** Docker

POSITIONS OF RESPONSIBILITY

- **Teaching Assistant :** Fundamentals of Computing I and II (CS111) (*Jan’23-Jul’23*)
- **Manager, Publicity and Public Relations (PG Wing)** : Election Commission IIT KANPUR (may’23-present)
- **Website Head: Hall 10 and CDAP Websites**
- **Orientation Team Memeber(OTM)** : Institute Counselling service (Jul’23)
- **Secretary :** International Relationship Wing of Academics and Career Council. (may’23-present)

RELEVANT COURSES

- **Mtech Courses :** Blockchain Technology and Applications, Modern Cryptography, Computer System Security, Practical Cyber Security for Cyber Practitioners, Hardware Security for IOT, Design for Security
- **Btech Courses :** Data Structures & Algorithms, Operating Systems, Computer Networks, Database Management System

ONLINE COURSES

- Completed **Machine Learning Specialization** certification from Stanford University by Andrew Ng.