SHIVANI KALE

shivanikale15797@gmail.com | +91-9962285526 | Solapur, Maharashtra - 413004 | linkedin.com/in/shivaniskale15797

SUMMARY

A Graduate student eager to contribute to team success through hard work, attention to detail and excellent organizational skills. Motivated to learn, grow and excel in the field of Cybersecurity. Experience in research related to Cryptography and its applications. Determined on understanding the subject of matter on a root level.

EXPERIENCE

Summer Research Intern, IIT Madras, Chennai *May 2019 - Oct 2019*
- Worked on Certificateless Proxy Re-encryption, its analysis and design.
- Researched on PKI based re-encryption and ID-based re-encryption as well.
- Studied attack scenarios on already existing schemes by identifying the weak problem of the scheme using oracles.

Project Trainee, IDRBT Hyderabad, Telangana *May 2018 - Jul 2018*
- Proposed a method for Iris Template security in the encrypted domain using Homomorphic ElGamal encryption scheme.
- Used Additive and Multiplicative ElGamal Encryption to store the templates and authenticate them in the encrypted domain.

Research Intern, IIITDM Kancheepuram, Chennai *Jun 2017 - Jul 2017*
- Research work in developing efficient Routing algorithms in order to reduce the search time and use less memory space.

PROJECTS

Implementation and Performance Analysis of Conjugate Gradient Method using Parallel Computation.
- This project focused on the implementation of the Conjugate Gradient Method to solve large systems of linear equations.
- The method was implemented in both serial and parallel fashion.
- OpenMP, MPI and CUDA along with concepts of High-Performance Computing were used to implement the method algorithm in parallel.
- The performance of the serial and parallel algorithm were analyzed while attempting to solve linear systems of different sizes on an increasing number of processors.

Secure Communication
- In this project, we implemented a variation of Bifid Cipher which was used to encrypt and decrypt messages exchanged between the client and server in order to secure the communication.
- The client and server were created on the same system with the help of sockets in Python.
- No cryptographic libraries were used while implementing the cipher.

EDUCATION

B.Tech + M.Tech (Dual Degree), Computer Engineering *Jul 2015 - Jun 2020*
Indian Institute of Information Technology, Design and Manufacturing(IIITDM) Kancheepuram, Chennai **GPA: 8.01**

SKILLS

Programming Languages: Python, C, C++, MATLAB
Tools: Wireshark, Keil software
OS: Windows, Linux
Concepts: Encryption, Decryption, Ciphers, Attacks on Cryptosystems, Blockchain and its proof of works, Computer Networks, Machine Learning algorithms, High-Performance Computing(OpenMP and MPI), MySQL

COURSE CERTIFICATIONS

- Introduction to Cybersecurity Tools and Cyber Attacks
- Cybersecurity Roles, Processes and Operating Security
- Cybersecurity Compliance Framework and System Administration
- Network Security and Database Vulnerabilities

ADDITIONAL INFORMATION

- Member of Robotics Club - 2016
- Volunteered at World Space Week organized by ISRO in 2016
- Coordinator of Robotics Club - 2017
- Languages - English, Hindi, Marathi(Native)