oatre@purdue.edu
(765) 409-4194

Om Atre

LinkedIn
Website

Education

Savitribai Phule Pune University — Pune, India
BE in Computer Engineering, CGPA: 8.39/10.0 — *Aug 2019 – May 2023*

- **Honors**: Data Science
- **Relevant Coursework**: Database Management System, Cloud Computing, Cyber Security and Digital Forensics, Software Testing and Quality Assurance, Computer Network and Security

Purdue University — West Lafayette, IN
Professional MS in Computer Science, GPA: 3.08/4.00 — *Jun 2023 – Jun 2025*

- **Concentration**: Information & Cyber Security
- **Past Coursework**: Foundational Principles of Information Security, Introduction to Systems for Information Security, Security Analytics, Information Security
- **Current Coursework (Spring 2024)**: Software Security, Network Security, Social Economic and Legal Aspects of Security

Internship

Armament Research and Development Establishment (DRDO) — Pune, India
Research Intern — *Feb 2022 – Apr 2022*

- Collaborated with a team of researchers to develop a framework for enhancing LAN security using SDN & virtualization technologies.
- Implemented intrusion detection algorithms using machine learning techniques to analyze network traffic & detect suspicious patterns.
- Configured SDN controllers, & virtualized network switches to manage flow rules & implement security policies.
- Conducted experiments to evaluate the framework's effectiveness in detecting & mitigating various network attacks [DDoS, Man in the Middle, & ARP spoofing].
- Presented research findings and published a detail report in the organization's internal library.

Publications

- **Customer Segmentation for Banking Strategy using Machine Learning**: Dec 2022
- **Design and Development of Dual-Polarized Orthogonal Cross Yagi antenna for the frequency range of 50MHz to 500MHz**: Aug 2021

Projects

- **STEALDBACK [Stealthy Backdoor Attack on Deep Learning Models through Trigger Pattern Injection and Defense Evaluation]**: Performed a backdoor attack by injecting a trigger pattern (a white 3x3 square at the bottom-right corner) into the dataset and training a model on the contaminated data. The attack's success rate was exceptionally high at 99.98%. To test the defense strategy, I created a function to generate images with a specific target label. As a basic defense mechanism, I implemented binary thresholding of images. This defense was evaluated against the backdoor attack & achieved a clean prediction success rate of 98.33%.
- **Cryptographic Vulnerabilities and Attacks**: Conducted cyber attack on dummy website server API's authentication, exploiting hash function vulnerabilities via MD5 collisions in Python. Wrote Python script to create programs w/ same MD5, different SHA-256 hashes, showcasing hash function understanding. Created Python script for CBC mode decryption, exploiting padding oracle vulnerability. Utilized Python & scapy to capture packets for WEP cryptanalysis & output original key through WEP key recovery.

Skills

1. Languages: C, C++, Python, Bash, HTML, CSS, Java, JavaScript
2. Technical:
   - Good understanding of Software Defined Networking & Virtualization.
   - Worked with Wireshark (packet capturing/analysis tool), Network Security tools, TCP/IP stack, & IT infrastructure.
   - Extensive experience with TensorFlow, Keras, PyTorch, Matplotlib, Generative Adversarial Networks, & Neural Networks (CNN, Recursive Neural Networks, & Recurrent Neural Networks).