Pragya Sharma

pragyasharma@vt.edu pragyasharmaa.github.io linkedin.com/in/pragya28 Google Scholar

Research Interests: 5G, IoT, Network Security, AI for Security, Reinforcement Learning, Federated Learning

Education

Virginia Tech — Arlington, Virginia, USA — Jan 2021 - Present
Ph.D. in Computer Engineering — *GPA: 4.0*
System and Software Security, Network Security, Fundamentals of Information Security, Blockchain Technologies

Indian Institute of Technology Bombay — Mumbai, India — Jul 2013 - Jun 2018
B.Tech. & M.Tech. in Electrical Engineering — *GPA: 8.36/10.0*
Fundamentals of Machine Learning, Markov Chains and Queuing Systems, Wireless and Mobile Communications

Internship

Kryptowire Labs — McLean, Virginia, USA — May 2022 - Aug 2022
Research & Development Intern

- Deployed the WAVE framework on a Kubernetes cluster and executed stress-testing experiments on WAVE persistent storage server to assess the scalability of the system in extensive deployment scenarios.
- Evaluated the performance of WAVE by analyzing metrics such as latency, CPU utilization, and storage size. Additionally, suggested alternative approaches for facilitating cross-domain interactions.

Publications

1. **5G-WAVE: A Core Network Framework with Decentralized Authorization for Network Slices**
   P. Sharma, T. Atalay, H. Gibbs, D. Stojadinovic, A. Stavrou and H. Wang
   IEEE INFOCOM 2024 - IEEE International Conference on Computer Communications

2. **FedMADE: Robust Federated Learning for Intrusion Detection in IoT Networks Using a Dynamic Aggregation Method**
   S. Sun, P. Sharma, K. Nwodo, A. Stavrou and H. Wang
   ISC 2024 - Information Security Conference

3. **Adaptive Flow-Level Scheduling for the IoT MAC**
   P. Sharma, J. Nair and R. Singh
   COMSNETS 2020 - International Conference on COMmunication Systems & NETworkS

Research Projects

Conflict Mitigation of xApps and rApps in 5G Open RAN Intelligent Controller (RIC) (Current)
Primary Researcher

- **Goal**: To design an AI-based conflict mitigation framework for xApps in 5G Open RAN RIC
- **Contribution**: Designing a multi-agent reinforcement learning (MARL) environment for mitigating conflicts among xApps in near-real-time RIC. Integrating xApps deployed on μONOS RIC with RL agents through side-car proxies that collect Key Performance Measurement (KPM) metrics from SD-RAN simulator.

5G-WAVE: Decentralized Authorization and Access of Network Functions (NFs) in 5G core
Primary Researcher

- **Goal**: To create a decentralized authorization framework for service access among 5G core VNFs
- **Contribution**: Integrated WAVE, a decentralized authorization mechanism to grant service access among 5G core VNFs. We removed the reliance of 5G core on OAuth 2.0, thus eliminating security vulnerabilities caused by a central authorization server. We demonstrated the functionality of 5G-WAVE by modifying OAI 5G core entities deployed on a Kubernetes cluster and validated the design scalability by measuring timing overhead in deployments with multiple slices.

Autonomous Cyber Agents for Security Testing and Learning Environments
Collaborating Researcher
- **Goal**: To develop an RL-based autonomous cyber range with varying degrees of fidelity to train red (attacker) and blue (defender) agents that dynamically adapt to network changes.
- **Contribution**: Worked towards building a high-fidelity network digital twin emulator by analyzing methods to clone softwares and known vulnerabilities from real networks. Built a test environment consisting of Metasploit, Kali Linux VMs, OpenVSwitch and Faucet SDN controller to demonstrate CAGE challenge scenarios.

Federated Learning-based Intrusion Detection in IoT Networks
Collaborating Researcher
- **Goal**: To develop a robust intrusion detection system for IoT networks using federated learning
- **Contribution**: We designed a dynamic aggregation method within the federated learning framework to address data heterogeneity from varying device vulnerabilities, significantly improving attack classification accuracy on real-world IoT traffic datasets.

Work Experience

Cadence Design Systems — Pune, India Jul 2018 - Dec 2020
Senior Design Engineer
- Worked on the development, optimization and benchmarking of IEEE 754 vector floating-point DSPs within the Tensilica family of MathX processors.
- Contributed to the optimization of Instruction Set Architecture (ISA) of Tensilica ConnX family DSP processors, focusing on achieving faster performance through the efficient utilization of VLIW slots. Additionally, benchmarked these cores in the context of communication and radar/lidar processing chains.
- Assisted in the development of the neural network (NN) library of the Tensilica HiFi4 DSP to enhance Automatic Speech Recognition (ASR) capabilities of voice-controlled digital assistants.

Awards

- IEEE INFOCOM Student Travel Grant (2024)
- Pratt Fellowship by ECE Department, Virginia Tech (2024)
- IIT Bombay Institute Organizational Color (2016)
- CBSE Merit Certificate for 12^{th} grade Maths and Sanskrit (99.9^{th} percentile) (2013)
- Government of India INSPIRE Scholarship (2013)

Course Projects

- Detecting price manipulation vulnerabilities in DeFi flash loan attacks using static taint analysis
- Feature-fingerprinting of SSH login attacks and countermeasures with honeypots
- Anomaly detection in network traffic data using deep Q-learning
- Securing private DNS records with DNSSEC and DANE
- Demonstrating key re-installation vulnerabilities in WPA2

Technical Skills

* **Software/Packages** - Kubernetes, Docker, OpenVSwitch, GNS3, Vagrant, Gymnasium, Wireshark
* **Languages** - C, C++, Python, Bash

Leadership/Volunteering Services

* **Student Volunteer** - srsRAN Project Fall Workshop (2024)
* **Technical Reviewer** - Journal of Computer Security (2024)
* **Technical Reviewer** - IEEE ICDCS (2024)
* **Technical Reviewer** - ESORICS (2024)
* **Campus Representative, Arlington** - Virginia Tech Graduate Student Assembly (VT-GSA) (2022)
* **President, Washington DC Chapter** - IIT Bombay Heritage Foundation (IITB-HF) (2022-24)
* **Web Nominee** - Hostel Affairs, IIT Bombay (2015-16)