

PRAGYA SHARMA

✉pragyasharma@vt.edu 🏠pragyasharmaa.github.io 🔗linkedin.com/in/pragya28 🎓Google Scholar

EDUCATION

Virginia Tech — Arlington, Virginia, USA

Jan 2021 - Present

Ph.D. in Computer Engineering

GPA: 4.0

Indian Institute of Technology Bombay — Mumbai, India

Jul 2013 - Jun 2018

B.Tech. & M.Tech. in Electrical Engineering

GPA: 8.36/10.0

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

Research Interests: 5G-RAN, 5G core, 5G security, Reinforcement Learning, Federated Learning, IoT

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

Mitigation of xApps and rApps Conflicts in 5G O-RAN Intelligent Controller (RIC) (Present)

- Built an emulation environment consisting of Metasploit, Kali Linux VMs, OpenVSwitch and SDN controllers to enable attack-defense plays for learning by red and blue agents.
- Working on simulating attacks on 5G core networks according to MITRE FiGHT attack TTPs to enable a learning environment for detection of advanced persistent threats (APTs).

5G-WAVE: Integrating WAVE with 5G core for decentralized authorization

- Designed and implemented a decentralized authorization framework for the 5G core service access among VNFs by utilizing WAVE to eliminate the security vulnerabilities caused by a central OAuth2.0 authorization server.
- Deployed the 5G-WAVE platform on a Kubernetes cluster with OpenAirInterface (OAI) entities as 5G VNFs. Modified the design to offload authorization among VNFs onto side-car proxies (SCPs) which enable service access by creation and verification of WAVE attestations.
- Measured time cost based performance of service operations in 5G-WAVE in network slice deployments to analyze latency overhead and scalability of the design with multiple slices.

Security Testing and Learning Environment for APTs in 5G Core

- Built an emulation environment consisting of Metasploit, Kali Linux VMs, OpenVSwitch and Faucet SDN controller to enable attack-defense plays for learning by red and blue agents.
- Worked on simulating attacks on 5G core networks according to MITRE FiGHT attack TTPs to enable a learning environment for detection of advanced persistent threats (APTs).

WORK EXPERIENCE

Cadence Design Systems — Pune, India

Jul. 2018 - Dec. 2020

Senior Design Engineer

- Worked extensively on development and optimization of IEEE 754 vector floating-point DSPs within the Tensilica family of MathX processors. Conducted comprehensive performance benchmarking of these DSPs using software examples compiled with both gcc and llvm C compilers.
- Contributed to the optimization and enhancement 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 - Maths and Sanskrit (for being in top 0.1% candidates) (2013)
- Government of India INSPIRE Scholarship (2013)

RELEVANT COURSES

- * **Security** - System and Software Security, Network Security, Fundamentals of Information Security
- * **AI** - Reinforcement Learning, Fundamentals of Machine Learning
- * **Others** - Blockchain Technologies, Markov Chains and Queuing Systems, Wireless and Mobile Communications

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

- * **Technical Reviewer** - Journal of Computer Society (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)