

# Aaditya Rengarajan

MS CYBERSECURITY CANDIDATE

New York University, NY

✉ +1 929-715-4928 | 📩 aaditya.r@nyu.edu | 🌐 www.aadi.zip | 🗃 aadityare | 📱 aadityarengarajan

## Research Interests

---

Post-Quantum Cryptography; Privacy-Preserving Machine Learning; AI Safety & Security; Threat Intelligence; Automated Reasoning; Federated Learning; Homomorphic Encryption; Capability-Based Security; Trusted Execution Environments; Cryptographic Protocols; AI Agent Security; Secure Systems Design; Critical Infrastructure Protection

## Education

---

### New York University

MS CYBERSECURITY

New York, NY, USA

September 2025 - present

- GPA: 4.0

- Courses: Application Security, Software Supply Chain Security, Post Quantum Cryptography

### PSG College of Technology (affiliated with Anna University)

Coimbatore, TN, India

2021 - 2025

BE COMPUTER SCIENCE & ENGINEERING

- Grade: First Class
- Thesis: Estimation of Warfarin Dosage using a Specialized XGBoost-based Pharmacogenomic Machine Learning Model and Evaluation using XAI
- Relevant Coursework: Cryptography, Machine Learning, Distributed Systems, Computer Networks

## Research Experience

---

### New York University - Secure Systems Lab

Brooklyn, NY

ADVISOR: PROFESSOR JUSTIN CAPPOS

2025

- Academic Paper: Prompt-Aware MCP Security: Using ShardGuard To Compartmentalize LLMs for Safer MCP Actions
- Implementing security isolation mechanisms using capability-based security
- Preparing manuscript for USENIX conference submission

### Intel Corporation

Bangalore, KA

MENTOR: MR. BALAKRISHNAN ANANTHANARAYANAN

2025

- Academic Paper: Constrained Deep Q-Learning for Optimal Offline Multi-Dimensional Bin Packing
- Developed Constrained Deep Q-Learning model for multi-dimensional bin packing optimization in semiconductor manufacturing, achieving 94.36% accuracy, proving improvement in efficiency and speed over baseline methods
- Implemented offline reinforcement learning algorithm using PyTorch, TensorFlow and OR-Tools to optimize foundry scheduling across around 50 constraint dimensions

### PSG College of Technology - Dept of CSE

Coimbatore, TN

2024, 2025

ADVISOR: DR. L. S. JAYASHREE

- Academic Papers: Estimation of Warfarin Dosage using a Specialized XGBoost-based Pharmacogenomic Machine Learning Model and Evaluation using XAI, SAABE: Secure Authentication and Avionic Broadcast Encryption
- Built XGBoost-based warfarin dosage prediction model achieving 94.36% accuracy; Published at ICMLC 2025

### PSG College of Technology - Dept of CSE

Coimbatore, TN

2022, 2024

ADVISOR: DR. G. R. KARPAGAM

- Academic Papers: Leveraging Detection Of Data Breaches By Applying Snowball Sampling, Enhancing Cybersecurity Resilience with CYBRANA: A Cyber YARA/YAML-Based Resilience Firewall Solution Applied with Next-Gen AI
- Designed CYBRANA, a YARA-rule firewall with AI-based threat detection; Published at IEEE CVMI 2024
- Developed data breach detection methodology using snowball sampling; Published at ICHPIC 2022

## Publications

---

**Aaditya Rengarajan**, Akshay Perison Davis, Navaneetha Krishnan K S, R Vishal and Subhasri Shreya S L, Jayashree L S. Estimation of Warfarin Dosage using a Specialized XGBoost-based Pharmacogenomic Machine Learning Model and Evaluation using XAI. 2025 International Conference on Machine Learning and Cybernetics (ICMLC).

**Aaditya Rengarajan**, Lohith Senthilkumar, Amitha Lakshmi Raj and Arun U S. Enhancing the Resilience of Privacy-Preserving Machine Learning using Adversarial Techniques. 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC).

Lohith Senthilkumar and **Aaditya Rengarajan**. FLARE: Federated Learning And Resilient Encryption for Firewalls. 2024 IEEE Pune Section International Conference (PuneCon). (*Mentored undergraduate researcher*)

**Aaditya Rengarajan**, Lohith Senthilkumar, Neelesh Padmanabh and Akhil Ramalingam. SHADOW: A framework for Systematic Heuristic Analysis and Detection of Observations on the Web. 2024 International Conference on Artificial Intelligence, Metaverse and Cybersecurity (ICAMAC). (*Mentored undergraduate researchers*)

**Aaditya Rengarajan**, G. R. Karpagam. Enhancing Cybersecurity Resilience with CYBRANA: A Cyber YARA/YAML-Based Resilience Firewall Solution Applied with Next-Gen AI. 2024 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI).

**Aaditya Rengarajan**, Mithilesh E N, Santhoshi R and Subhasri Shreya S L, G. R. Karpagam. Leveraging Detection Of Data Breaches By Applying Snowball Sampling. 2022 International Conference on High Performance and Intelligent Computing (ICHPIC).

## Awards & Honors

---

2025	NYU Graduate Merit Scholarship, New York University Cybersecurity Leadership Award, PSG College of Technology	\$8,000
2024	FinTech Award, FinTech Festival India	\$1,100
2021	Professional Development Grant, PSG College of Technology	\$225

## Presentations

---

### INVITED TALKS

Fall 2024. *SHADOW: A Framework for Dark Web Monitoring Using Named Entity Recognition and Threat Intelligence*. Invited talk: 3rd Annual International ISC2 Chapter Conference, New Jersey, USA.

Summer 2024. *Security Challenges in Aviation and Aerospace Systems*. Invited talk: OWASP Coimbatore Chapter, Coimbatore, Tamil Nadu, India.

### CONTRIBUTED PRESENTATIONS

**Intel Corporation**. 2025. Delivered a technical presentation on Agentic AI, covering secure coding practices and its use in full factory scheduling and automation of foundry processes. Industry technical talk: Intel, Bengaluru, Karnataka, India.

**NYU MakerSpace**. 2024. Contributed to a hands-on *Cyber Security 101: Capture the Flag* seminar, introducing students to practical web security concepts through interactive challenges. Cross-departmental seminar: New York University, New York, NY, USA.

**Department of CSE, PSG College of Technology**. 2024. Contributed to a workshop on open source intelligence (OSINT) for students. Intercollegiate workshop: Department of CSE, PSG College of Technology, Coimbatore, TN, India.

**OWASP Coimbatore Chapter**. 2024. Contributed to a workshop with a talk on aviation cybersecurity, and ethical hacking of aerospace systems. OWASP Coimbatore Chapter, Coimbatore, TN, India.

**Department of CSE, PSG College of Technology**. 2023. Contributed to a workshop with a talk on aviation cybersecurity, and ethical hacking of aerospace systems. Intercollegiate workshop: PSG College of Technology, Coimbatore, TN, India.

**Department of CSE, PSG College of Technology.** 2023. Conducted a 2-day departmental seminar for students and faculties to introduce them to basic Cybersecurity from a technical aspect. Departmental seminar: Department of CSE, PSG College of Technology, Coimbatore, TN, India.

**Department of CSE, PSG College of Technology.** 2022. Conducted a 2-day departmental seminar for students and faculties to introduce them to basic Cybersecurity from a technical aspect. Departmental seminar: Department of CSE, PSG College of Technology, Coimbatore, TN, India.

## Teaching Experience

Spring 2026 Application Security, Course Assistant New York University

## Mentoring

- |           |   |
|-----------|---|
| 2024-2025 | <b>Lohith Senthilkumar</b> , Research, Department of CSE, PSG College of Technology |
| 2023-2024 | <b>Neelesh Padmanabh</b> , Research, Department of CSE, PSG College of Technology   |
| 2023-2024 | <b>Akhil Ramalingam</b> , Research, Department of CSE, PSG College of Technology    |

## Professional Experience

- |           |  |
|-----------|--|
| 2026      | <b>Graduate Course Assistant, Application Security</b> , Dept. of Cybersecurity, New York University |
| 2025      | <b>Deep Learning R&amp;D for Operations Research (Intern)</b> , Intel Foundry, Intel Corporation     |
| 2024      | <b>Security Operations Intern</b> , Indian Space Research Organization                               |
| 2022-2023 | <b>Security Software Engineer (Intern)</b> , Tactical Cyberange Simulations                          |
| 2019-2021 | <b>Data Science (Freelance Engineering)</b> , EQUATE Petrochemical Company                           |

## Outreach & Professional Development

## SERVICE AND OUTREACH

- |             |   |       |
|-------------|---|-------|
| 2023 – 2024 | <b>Students' Union, Technical Project Planner</b>               | India |
| 2021 – 2025 | <b>Institution's Innovation Council, Lead Software Engineer</b> | India |
| 2021 – 2022 | <b>Aeromodelling Club, PSGCT, Research Associate</b>            | India |

## PROFESSIONAL MEMBERSHIPS

Member: IEEE, OWASP, ISC2

## SYSTEMS DEPLOYED

ASTRA: A Cyber-Threat Intelligence Framework for Advanced Security Threat Response and Analysis. System deployed at National Remote Sensing Centre (NRSC, ISRO), 2024 at Hyderabad, India.

## References

**Prof. G. R. Karpagam Manavalan**

Department of Computer Science & Engineering, PSG College of Technology, India  
Email: grk.cse@psgtech.ac.in

**Prof. G. Sudha Sadasivam**

Head, Department of Computer Science & Engineering, PSG College of Technology, India  
Email: [hod, gss].cse@psgtech.ac.in

*Other references available upon request.*