

Raj Patel

rpatel627@gatech.edu | (727) 558-3016 | Atlanta, GA | [linkedin.com/in/rajpatel627](https://www.linkedin.com/in/rajpatel627)

Graduate student at Georgia Tech with hands-on experience in malware reverse engineering, threat intelligence, and network security. Skilled in SIEM platforms (Splunk, ELK), IDS tools (Suricata, Snort), and network analysis with Wireshark. Experienced with digital forensic support, detection alerts, and security engineering concepts.

EDUCATION

- **Georgia Institute of Technology** *Atlanta, GA*
- *Master of Science, Computer Engineering* **December 2026**
- *Bachelor of Science, Computer Engineering* **December 2024**

SKILLS

- **Certifications:** Security+ (*Expected 2025*), HackTheBox SOC Analyst, AWS Cloud Practitioner (*In-Progress*)
- **Programming:** Python, C++, Java, C, HTML, CSS, MATLAB, JavaScript, R
- **Development:** IDA Pro, GitHub, Assembly, Ollydbg, Kubernetes, Docker, Virtualization (VMWare, VirtualBox), VHDL, Verilog, Git, Flask, CUDA, Hadoop, Spark, Linux
- **Tools and Techniques:** SIEM (Splunk, ELK), IDS (Suricata, Snort), Wireshark
- **Knowledge Areas:** Compliance frameworks (NIST, ISO), MITRE ATT&CK
- **Relevant Coursework:** Enterprise Security Management, Malware Reverse Engineering, Advanced Malware Analysis, Computer Security, Introduction to Networking, Cybersecurity in Drones
- **Extracurricular:** GreyHat (GT cyber), PicoCTF

WORK EXPERIENCE

- **Pramukh Transport Ltd.** **August 2022 – January 2025**
- *Cyber Risk Analyst, Part-time* *Nakuru, Kenya*

- Developed and analyzed the company's threat profile enabling leadership and stakeholders to understand the cyber risks and implications of conducting business digitally and informing strategic risk management decisions.
- Maintained risk register entries to document vulnerabilities and align with business risk appetite.

- **Akshar Auto Spare House** **June 2020 – August 2020**
- *IT Technician, Intern* *Nakuru, Kenya*

- Resolved network and OS vulnerabilities and strengthened endpoint resilience to improve user satisfaction by 20%.

PROJECTS

Research Team: Cyber-physical Systems

- Conducted threat modeling of cyber-physical systems to identify potential attack vectors, then presented findings and advised on risk mitigation strategies through 2 papers and 3 presentations.

Malware Reverse Engineering

- Reverse engineered 5+ malware samples (DOS-7, Michelangelo, SQLSlammer, Lucius, Harulf) using Assembly, IDA Pro, Ollydbg, and Wireshark to identify IOCs and produced detailed technical reports with annotated disassembly and behavior analysis

ML-Based Network Intrusion Detection System

- Developed a defense system that removed hidden backdoor attacks using machine unlearning, leveraging scikit-learn, Pandas and NumPy for model training and evaluation.
- Supported incident response by integrating Suricata rules into ML-based IDS detection accuracy to 100% on SSH brute-force attempts.

AI Drone Anomaly Detector

- Integrated a Python/C++ KNN ML model into ArduPilot firmware to detect tampered, or faulty IMU data, successfully detecting 95% of injected anomalies in SITL simulations

Web Application Development

- Developed 4 secure versions of a scalable cloud-based web photo gallery application integrating IAM, REST APIs, EC2, SQL, Docker, automated CI/CD pipelines, and cloud-based deployments using AWS and Kubernetes.
- Implemented IAM policies to enforce cloud security in AWS S3, cutting exposure to misconfigurations by 30%.

Android Game Application

- Collaborated with 3 developers to review code, exchange technical feedback, and align DevSecOps practices, employing Agile Methodology over 5 sprints.