Aarnav Singh

+91-9971506703 | aarnavujji@gmail.com | LinkedIn | GitHub | Portfolio

Professional Summary

Final-year B.Tech Computer Science & Engineering student (Cybersecurity specialization) with hands-on experience in intrusion detection, adversarial machine learning, and Zero-Trust security architecture. Co-author of a research paper currently under review at the *Journal of Information Security and Applications* (Elsevier), demonstrating a reduction in adversarial-attack bypass rates from 65% to 2.2% using Zero-Trust contextual policies.

Education

SRM University India
B.Tech in Computer Science & Engineering with specialization in Cybersecurity *2022 – 2026*
- GPA: 7.74/10

Experience

HCLTech – Intern May 2024 – July 2024
Noida, India
- Built foundational skills in enterprise network security and perimeter security – including firewalls, network segmentation, and threat mitigation strategies.
- Gained hands-on understanding of Microsoft Azure cloud infrastructure while supporting network and security operations.
- Applied Python for DevSecOps automation, including security tooling configuration and codebase review to support automated security workflows.

Projects

Adversarial Attack Detection in Zero-Trust Networks Jan 2026
- *GitHub:* github.com/Aarnav-Singh/adversarial-ml-security-framework
- Built a six-layer Zero-Trust network security system in Python/PyTorch combining ML-based intrusion detection with a context-aware policy engine.
- Trained neural network classifiers on UNSW-NB15 and CICIDS-2017, achieving 90.7% and 99.9% accuracy across 5 random seeds.
- Implemented domain-constrained FGSM/PGD adversarial attacks and reduced system bypass rates from 65% to 2.2% via Zero-Trust contextual signals – without model retraining.
- Co-authored a research paper based on this work, currently under review at the Journal of Information Security and Applications (Elsevier).

Hybrid Behavioral Intrusion Detection System Feb 2026
- *GitHub:* github.com/Aarnav-Singh/Hybrid-Behavioral-Intrusion-Detection-System
- Designed and developed a full-stack hybrid intrusion detection system combining rule-based detection with Isolation Forest-based anomaly detection for behavioral threat analysis.
- Built a real-time React dashboard using WebSockets and REST APIs for live threat visualization and alerting.
- Integrated Elasticsearch for centralized log indexing and threat-event correlation, and deployed Prometheus for monitoring detection latency and system performance.
- Containerized the full system using Docker to simulate a scalable deployment environment aligned with Zero-Trust and modern security monitoring principles.

Technical Skills

Security & Monitoring: Intrusion Detection Systems (IDS/IPS), SIEM Concepts, SOAR, Log Analysis, Incident Response, Threat Detection & Cyber Threat Intelligence (CTI), Vulnerability Assessment, MITRE ATT&CK Framework

Machine Learning: Adversarial Machine Learning, Anomaly Detection, Isolation Forest, Feature Engineering, ROC Curve, Confusion Matrix

Networking & Zero-Trust: TCP/IP, DNS, VPN, Network Segmentation, Firewalls, Routing & Switching, Zero-Trust Architecture (ZTNA), SASE, Secure SD-WAN, NAC

Tools & Platforms: Elasticsearch, Wireshark, Nmap, Nessus, Metasploit, FortiGate, Kali Linux, Web Application Firewalls

Cloud & Development: Microsoft Azure, AWS, IAM, DevSecOps, Linux, Windows, Python, PyTorch, Docker, React.js, REST APIs, WebSockets

Certifications

ISC2 – Certified in Cybersecurity (CC)

Fortinet – Fortinet Certified Associate (FCA)

Fortinet – Fortinet Certified Fundamentals (FCF)

NPTEL – Advanced Computer Networks

Deloitte Australia (Forage) – Cyber Job Simulation

Leadership & Activities

Volunteer – Purvanchal Vikas Foundation June 2024 – July 2024
Noida, India
- Supported outreach initiatives and beneficiary enrollment programs.

Core Member & Event Host – Gamer's Creed Esports Club
Ghaziabad, India
- Hosted and coordinated college-level esports events.