K. VIJAY PRATHAP REDDY

Grand Rapids, MI • (616) 500-4832
vijayreddypr999@gmail.com • linkedin.com/in/vijay-prathap-reddy/

SUMMARY

Results-driven Security Analyst with 3+ years of experience and Master's candidate in Cybersecurity with SOC expertise, specializing in malware analysis, AI-driven detection frameworks, and network security. Proven ability to build automated threat identification systems that enhance security resilience. Proficient in penetration testing, cryptography, machine learning, and IoT security. Hands-on experience in threat detection with academic rigor in data analysis and classification using AI/ML for cybersecurity. Flexible for shift-based schedules and open to onsite/remote roles across the U.S.

SKILLS

- **Core Focus:** SOC operations, Malware Analysis, Network Security, AI-Driven Detection, Penetration Testing.
- **Cybersecurity Domains:** Network Security, Cryptography (RSA/ECC/AES), Ethical Hacking, IoT Security, Secure Software Engineering, Web Application Security (XSS, SQLi, CORS).
- **Machine Learning:** Python (Pandas, scikit-learn, Matplotlib), Regression Models, Decision Trees, Random Forest, Data Preprocessing, Model Evaluation (F1-score, Precision).
- **SecOps:** Splunk Enterprise Security, Microsoft Defender XDR, Anomali Threatstream, Palo Alto NGFW, Tanium.
- **Programming:** Python, KQL (Kusto), SPL (Splunk), PowerShell, Bash.
- **Pen-Testing:** Metasploit, Burp Suite, Kali Linux, Hydra, John the Ripper, Wireshark, Nmap, tcpdump, Nessus, Snort.
- **Malware Analysis and Forensics:** ANY.RUN, Cuckoo Sandbox, FLARE VM, Volatility, Autopsy, Netcat.
- **Networking:** Routing/Switching, VLANs, VPN, IDS/IPS, GNS3, Mininet, Cisco Packet Tracer.
- **Cloud/IAM:** Microsoft Azure AD (Entra ID), Microsoft Cloud App Security (MCAS), SailPoint.

EXPERIENCE

Grand Valley State University, Michigan • Cybersecurity Research Assistant *08/2024 - Present*

- **Detecting Rogue Switch and Device Behaviour Using Network Anomalies in LAN:** European Conference on Cyber Warfare and Security (ECCWS), 2025. Published. Open paper: https://doi.org/10.34190/eccws.24.1.3705.
- **Lightweight SME Solution (Near Publication):** Built a real-time monitoring system using Mininet and Open vSwitch with Bash scripting to track topology changes, unknown devices, and ARP inconsistencies. Implemented three detection rules (port/link anomalies, MAC-IP mismatches, spoofing behavior) reducing false positives through automated email alerts. Validated framework in simulated SME environments, enabled threat containment with minimal infrastructure.
- **Dynamic Network Sketches — Research Project (In Progress):** Data processing and implementation of sketches (SSVS, SSVS2, HyperLogLog); comparisons on flow size/flow spread (accuracy, memory, speed); lightweight approach for routers/switches with limited memory/CPU to detect unusual flow size and flow spread bursts.

GVSU Surplus Store, Michigan • IT Student Worker *11/2024 - Present*

- Refurbished and troubleshot cross-platform hardware (Windows/Linux/macOS/Unix); executed system imaging/configurations for device resale with quality control.
- Streamlined inventory tracking through automated documentation, improving operational efficiency by 30%.

Grand Valley State University, Michigan • Cybersecurity Teaching Assistant *01/2025 - 04/2025*

- Facilitated static/dynamic malware analysis labs using FLARE VM/Cuckoo Sandbox; developed hands-on exercises for threat detection, binary analysis, and secure coding (XSS/SQLi).
- Designed and evaluated practical modules on network behavior and response strategies, enhancing student readiness for real-world security challenges.

Fidelity National Financial, India • Security Analyst *02/2022 - 12/2023*

- Reduced Incident Response times by performing thorough investigations using Splunk ES, Microsoft Defender XDR, Tanium, and ticketing tool ServiceNow; integrated IOCs using Anomali ThreatStream to boost detection accuracy.
- Mitigated phishing/malware via Microsoft Defender XDR; enforced least-privilege access using Azure AD and SailPoint.
- Enhanced visibility using Palo Alto Next-Gen Firewalls; performed proactive Endpoint-Threat Hunting with KQL (Kusto).
- Strengthened Cloud Security Posture for regulatory compliance via Microsoft Cloud App Security.

ACADEMIC PROJECTS

Detecting Rogue Switches in LAN Using AI (Capstone)

- Hybrid framework merging Cisco Layer 2 defenses (DAI for ARP validation, Root Guard for BPDU blocking, Port Security with sticky MAC) and logistic regression classifiers targeting ARP spoofing, MAC flooding, and root bridge attacks.
- Attack simulation via GNS3 topology using Cisco switches, Kali Linux (Ettercap/Macof), and Windows VMs; trained models on structured metadata (BPDU priority, MAC variation, port mapping).
- **Results:** Static defenses blocked attacks in real-time; AI models achieved 100% F1-score across all threat scenarios.

IoT Multi-Layer Security Framework

- **Perception Layer:** TLS/ECC for encrypted sensor-gateway communication.
- **Network Layer:** Fog computing + blockchain logging for tamper-proof traffic records.
- **Application Layer:** RBAC + time-segmented algorithm (4 daily intervals) to detect DoS anomalies.
- **Outcome:** Addressed 100% of 12 IoT security requirements; surpassed 14 frameworks in layered protection.

Bengaluru House Price Prediction (ML)

- **Engineered Pipeline:** Missing value imputation, one-hot encoding, MinMax scaling, and outlier removal. Optimized Random Forest (vs. Linear Regression/SVR) achieving lowest RMSE; validated generalizability with synthetic cases.

EDUCATION

Grand Valley State University, Michigan • Master's in Cybersecurity *12/2025*
Sri Venkateswara University, Tirupati • Bachelor's in Electronics and Computer Science *10/2020*

CERTIFICATIONS

- EC-Council Certified Ethical Hacker (CEH v11)
- Microsoft Security, Compliance, and Identity Fundamentals (SC-900)
- SOC Experts - Certified Security Operations Centre (SOC) Analyst