GORLA PAVAN KUMAR

(913)-413-5011 | gorlapavan12345@gmail.com

PROFFESIONAL SUMMARY

Detail-oriented and self-motivated Software Engineer with hands-on experience in the full software development lifecycle, object-oriented programming, automated testing, and Agile delivery. Skilled in developing scalable, maintainable applications using Java, Python, SQL, and cloud technologies such as AWS and Azure. Strong collaborator with experience supporting high-availability systems, CI/CD pipelines, and version control. Known for rapid learning, clear communication, and delivering measurable value through well-tested code.

TECHNICAL SKILLS

- **Programming Languages:** Java, Python, PowerShell, JavaScript, C, SQL, HTML, CSS
- **Security & Compliance**: Risk Assessment, Vulnerability Management, Security Policy, Security Awareness Training
- **Tools & Platforms:** AWS, Azure, Nessus, Elastic Stack, Wireshark, Nmap, Burp suit, Selenium, TestNG, VirtualBox, Cisco Packet Tracer, MySQL, Eclipse, PyCharm, Notepad
- **QA & Testing:** Manual/Automated Testing, CI/CD, Agile Methodologies, Test Case Development
- **Cloud & Networking**: AWS, Azure, SaaS, PaaS, IaaS, Cloud Security Architecture
- **Frameworks/Tools:** Selenium, TestNG, Git, Postman, Node.js (familiar), Jenkins, Jira, TestRail, Xcode (familiar)
- **Microsoft tools:** Excel, PowerPoint, Teams
- **Methodologies**: Agile, SDLC, ITIL (familiar)
- **OS & Systems**: macOS, Windows, Linux (Ubuntu), Core OS Concepts
- **Soft Skills**: Cross-Functional Collaboration, Technical Writing, Agile Methodologies, Critical Thinking

EDUCATION

Master of Science in Cybersecurity and Information Assurance **Jul 2023 – May 2025**
University of Central Missouri
GPA: 3.8
Relevant Coursework: Cloud Computing, Cloud Security, Network Security, Software Engineering, Cybersecurity Policy, Threat Intelligence, Design of Cryptography, Information Assurance

WORK EXPERIENCE

Cognizant Technology Solutions
Cybersecurity analyst Intern **Jan 2022- July 2023**

- Monitored and analysed security logs from SIEM tools (Elastic Stack, Splunk), firewalls, and endpoint systems to detect potential threats.
- Performed real-time incident triage and responded to alerts following internal security protocols; escalated confirmed threats to Tier 2 with detailed documentation.
- Conducted vulnerability assessments using Nessus; supported remediation tracking in coordination with IT teams.
- Configured and tested security controls across AWS and Azure infrastructure in line with ISO 27001 and NIST guidelines.
- Managed incident tickets and provided first-line support for security issues, tracking resolution status across teams.
- Assisted in asset tracking and inventory validation for enterprise security systems.
- Authored and maintained technical documentation, including incident reports and policy procedures.
- Proactively researched emerging threats and AI-driven detection techniques to enhance security posture.

Cognizant Technology Solutions, Quality Assurance Tester **July 2021-July2022**

Client: London Stock Exchange Group (LSEG)

Tech Stack: Java, Selenium, Postman, Jira, TestRail, Confluence, AWS, Agile Methodologies, TestNG, Git, Rest APIs

- Designed and implemented **automated testing solutions** using **Selenium, Java, and TestNG**, improving efficiency.
- Led **cross-functional collaborations** for LSEG projects, reducing testing time by **40%**.
- Utilized **JIRA, Confluence, and Git** for test case management, progress tracking, and reporting.
- Integrated **CI/CD pipelines** and **Jenkins** for automated testing, ensuring seamless deployment.
- Migrated testing processes to **AWS cloud**, enhancing scalability and product support.
- Managed **QA signoff and release activities** for LSEG Workspace application

Programmer Analyst Trainee

Cognizant Technology Solutions | Remote | **Jan 2021 – June2021**

- Assisted in **software development and testing**, gaining hands-on experience in SDLC.
- Assisted in **designing, developing, and testing** software applications to meet business requirements.
- Gained hands-on experience with **Agile methodologies** and participated in **scrum meetings**.
- Developed **test cases** and performed **unit testing** to validate software functionality.
- Collaborated with **senior developers** to debug and resolve software issues, improving system reliability.
- Documented and analysed test results, ensuring adherence to **SDLC best practices**.
- Provided support for **production deployment** and post-release maintenance.

LEADERSHIP EXPERIENCE

Chairperson | SAE Club, VBIT | **Jun 2021 – Mar 2022**

- Led a **team of 50+ members**, organizing technical workshops and cybersecurity awareness programs.

PROJECTS

Elastic Stack SIEM Setup

Configured a centralized SIEM solution using Elasticsearch, Logstash, and Kibana (ELK Stack) for real-time log aggregation, parsing, and visualization. Developed custom dashboards and alerting rules to detect suspicious activities. Enhanced incident detection capabilities across multiple data sources.

Task Management CLI App (Agile Sprint Tracker)

Developed a Python-based command-line application to manage Agile tasks and sprints. Implemented features for creating user stories, assigning tasks, tracking progress, and generating sprint reports. Emphasized Agile principles and team collaboration in a simulated development workflow.

Tools: Python, SQLite, Click, Git, Linux Terminal

Network Traffic Analysis and Threat Detection

Utilized Nmap and Wireshark to inspect live network traffic for potential anomalies and unauthorized access attempts. Captured and decoded packets to analyse protocols like TCP/IP, DNS, and HTTP. Applied filtering techniques to trace root causes of suspicious activities and detect intrusions.

Secure Cloud Networking in AWS

Designed and deployed a secure Virtual Private Cloud (VPC) architecture with public/private subnets, NAT gateway, and tightly scoped security groups. Implemented IAM roles and policies to restrict access and enforce least privilege. Validated configuration against AWS security best practices.

Cloud Monitoring and Incident Automation System

Tools: AWS CloudWatch, EC2, Lambda, SNS, Python, CloudTrail, S3

Implemented a scalable cloud monitoring solution using AWS CloudWatch to track EC2 health and service metrics. Set up SNS

notifications for threshold breaches. Integrated AWS Lambda to automate log parsing and self-healing actions. Used CloudTrail for auditing and S3 lifecycle policies for secure log storage.

Web Automation Projects

Developed Java-based Selenium automation scripts for data scraping and functional testing of web applications, including a hospital locator and Quora content retriever. Used TestNG framework for test execution and validation, enhancing data collection accuracy and testing speed.

AI in Cybersecurity Research

Published academic research exploring the application of artificial intelligence in threat detection, phishing analysis, and malware classification. Evaluated machine learning models for predictive cybersecurity defense and contributed findings to cybersecurity communities.

Automated Payroll System with GPS and Image Verification

Designed a payroll management application integrated with GPS location tracking and image capture. Automated attendance tracking, payroll computation, and reporting. Enhanced transparency and security of workforce management, particularly for remote employees.

Web Application Security Testing Using Burp Suite

Performed end-to-end penetration testing on a custom-built web application. Intercepted HTTP traffic using Burp Suite to uncover vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and weak authentication mechanisms. Automated scanning using Burp Scanner and manually tested for business logic flaws.

Security Monitoring & Incident Response

Investigated and triaged security alerts using Elastic Stack, escalating confirmed incidents per SOC protocol. Performed log collection, packet analysis (Wireshark), and threat containment actions during internships. Familiarity with key Windows security event IDs and log formats

SIEM & Vulnerability Tools

Proficient with Elastic Stack SIEM setup (ELK), including custom alerting and dashboards. Conducted vulnerability assessments with Tenable/Nessus, delivering detailed remediation reports. Used regex and logic fluently to detect anomalies in logs and automate alerting rules

Threat Intelligence & Research

Utilized OSINT tools to investigate suspicious indicators (hashes, IPs, domains) and enrich alerts. Academic research in AI-driven threat detection and malware classification. Regularly track TTPs from MITRE ATT&CK and emerging threat feeds to inform investigations

CERTIFICATIONS

- **CompTIA Security+**, Candidate ID: COMP001022619499 (Oct 2024)
- **CompTIA IT Fundamentals+**, Candidate ID: COMP001022619499 (Sep 2024)
- **AWS Academy Cloud Security Foundations**
- **PCAP: Programming Essentials in Python** (Python Institute)
- **Cybersecurity Essentials** (Cisco)
- **Try Hack Me Pre Security Certificate** – Completed hands-on labs in cybersecurity fundamentals
- **AWS Certified Solutions Architect – Associate** | Amazon Web Services (AWS) | Issued: April 2025