Krishna
B.Tech. (Computer Science Engineering Specialization in Cybersecurity and Digital Forensics)
Contact no. +91 9350695701
Email: singlak999@outlook.com
LinkedIn: https://www.linkedin.com/in/krishna-k-21117b219/
GitHub: https://github.com/singlak999
Portfolio: https://krishnagupta.live

Education

- **B.Tech** | Vellore Institute of Technology (CGPA 8.82) 2021- 2025
- **Intermediate** | Daffodil Public School (CBSE 78.8%) March 2021
- **Matriculate** | Scholars Rosary Sr. Sec. School (CBSE 93.6%) March 2019

Experience

- **Data Analyst Intern** | Yojak, Bizcon innovations Pvt. Ltd September 2023 –November 2023
  - Enhanced decision-making speed by 25% for the analytics team through a comprehensive database of 500,000+ rows.
  - Analyzed over 100 local, national, and global market trends to identify potential threats and opportunities, driving strategic decision-making which increased market share by 15% within one fiscal year.
- **Cloud Security Associate** | Unisys Global Services January 2025 - Present
  - Analyzed the architecture of Rubrik security cloud VM Ransomware detection and data recovery.
  - **Leveraged tools like [e.g., Tenable, Microsoft Defender, Key Caliber, Splunk]** to drive a Continuous Threat Exposure Management (CTEM) framework, enabling real-time risk assessment and prioritization of threats.
  - Researched and implemented **Post-Quantum Cryptography (PQC)** algorithms to enhance resilience against quantum computing threats, focusing on NIST-recommended lattice-based cryptosystems.
  - **Executed controlled simulations of cyber threats** such as Ransomware encryption, DDoS floods, SQLi payloads, and credential brute-force attempts to test incident response effectiveness and harden system security.

Projects

- **Autonomous Multi-Agent SOC AI System on Azure.**
  - Architected a fully autonomous SOC AI pipeline on Microsoft Azure AI Foundry, orchestrating 4 specialised agents (Triage, Investigation, Comms, Remediation) to investigate and close Microsoft Sentinel incidents end-to-end without human intervention for standard-tier assets.
  - Automated MITRE ATT&CK mapping, Crown Jewel asset classification, and confidence-scored threat verdicts using real-time KQL queries against Azure Log Analytics, correlated with Entra ID Protection risk scores and MDE device timelines.
  - Executed autonomous remediation via Microsoft Graph API and MDE REST API — account disabling, session revocation, MFA re-registration, and IP blocking — governed by a hard policy engine the LLM cannot override.
  - Deployed containerised agent on Azure Container Apps (VNet-injected) with Cosmos DB state persistence, Logic App webhook trigger, and a single-script Bicep + Docker CI/CD pipeline.
- **Facial recognition-based surveillance system using Raspberry-PI.**
  - Boosted situational awareness for operational teams with algorithms achieving 95% accuracy in real-time tracking.
- **RASA based WhatsApp Chatbot.**
  - Deployed a RASA-based WhatsApp Chatbot with NLP capabilities, resulting in a 50% reduction in customer service response time.
  - Increased customer satisfaction ratings by 20% through sentiment analysis integrated into the RASA-based WhatsApp Chatbot.
- **Network Traffic Monitoring (Controlled Environment).**
  - Spearheaded the design and implementation of a robust network traffic monitoring system using ARP, enhancing visibility of network activities and reducing troubleshooting time by 40% in a controlled lab environment.
  - Deployed comprehensive analysis of network traffic behavior, revealing 10 key data flow bottlenecks; implemented targeted solutions that enhanced throughput by 40% and decreased packet loss rates by 15%.
- **Cyber Recovery Framework for Ransomware Resilience**
  - Designed and implemented a cyber recovery framework to defend against ransomware attacks in hybrid environments using Cyber Recovery Tool Security Cloud integrated with VMware vSphere.
  - Performed periodic VM snapshots, automated anomaly detection (entropy/file change-based), and executed instant recovery from encrypted states.
  - Achieved full restoration of business services within 5 minutes after attack simulation, ensuring operational continuity and integrity validation.
- **Exposure-Driven Threat Analytics via CTEM Pipeline**
  - Built a Continuous Threat and Exposure Management (CTEM) pipeline utilizing Azure Functions, Data Lake, Data Factory, and SQL Database to automate ingestion and transformation of asset vulnerability data.
  - Integrated third-party tools (Attack Surface Monitoring Tool & Risk-Based Exposure Management Tool) to assess public-facing risks and prioritize asset protection based on business criticality.
  - Enabled SOC teams to visualize real-time exposure trends and automate ticket escalation in ServiceNow through Sentinel + Logic Apps workflow.

- **Cloud-Native Simulation Lab for Attack Detection Engineering**
  - Created a secure attack lab using Kubernetes, Docker, and Azure VMs to deploy vulnerable apps (DVWA, custom React apps) and simulate advanced threats (DDoS via Slowloris, SQLi, lateral movement).
  - Developed detection logic using Sysmon + Azure Sentinel with custom KQL analytics rules, covering behavior-based anomalies, long-lived TCP connections, and unauthorized service installations.
  - Improved alerting precision and reduced false positives through real-world validation, enhancing response agility and SIEM rule quality.
- **Real-Time Phishing Detection Proxy Server**
  - Designed and implemented a proxy server to intercept HTTP/HTTPS traffic and extract URLs for analysis.
  - Developed and integrated a custom machine learning model to classify URLs as phishing or legitimate with real-time blocking capability.
  - Enhanced network security by preventing malicious access attempts and ensuring seamless user experience without latency issues.

Skills

- **Computer languages**: Python, Java, R, C++, Dart
- **Packages**: NumPy, Pandas, OpenCV, Flask, SQL, Rasa, Flutter
- **Skills**: Object oriented programming, Data Structures, Penetration Testing, Binary Exploitation, Linux, Cloud Computing, Firebase, Cryptography, Microsoft power automate, Microsoft Azure, AWS, Kubernetes, Post quantum cryptography
- **Tools:** Cribl, Splunk, Wireshark, Burp Suite, SNORT, Nginx, Git, Opensearch, Logstash, Hydra, MetaSploit, KeyCaliber, Spidersilk, Microsoft Sentinel, Rubrik security cloud, V-Sphere, Suricata, Sysmon, IDPS

Awards / Scholarships / Academic Achievements

- A book chapter accepted titled "IoT based Intelligent Home Automation System using IFTTT with Google Assistant", Intelligent Systems in Electrical Engineering, Springer, June 2023.
- Won the "Design Thinking Challenge", organized by the School of Mechanical Engineering (SMEC), VIT-AP University during 3rd May – 5th May 2023.
- Got selected for Amazon Machine Learning Summer School-2024.
- Represented India at _VOIS international hackathon by Vodafone.

Positions of Responsibility & Extra Curriculars

- **Technical Team Lead and Treasurer** | LIT-Data Analysis Club
- **Technical Team Lead** | Next-Gen Cloud Club
- **Technical Team Member** | Computer Society of India

Certificates and Licenses

- **Oracle Cloud Infrastructure DevOps Professional | Link**
- **Rafay Certified GPU Cloud Professional | Link**
- **Claude Certified Architect| Link**