Syed Muhammad Mojiz Ali Zaidi

+90-501-161-3938 | zaidimojiz4@gmail.com | LinkedIn | github.com/zaidi14 | Kayseri, Türkiye

Summary

ISC² Certified in Cybersecurity (CC) security engineer and Computer Engineering undergraduate (Abdullah Gül University, 2027) with hands-on experience in **cloud infrastructure hardening**, **network segmentation**, and **API security**. Architected and deployed an isolated deception environment on **Azure** end-to-end; hardened production **healthcare APIs** under **GDPR** and **HIPAA**; designed **zero-trust** edge enforcement systems from hardware level upward. Actively building **IaC** and **container security** depth (KodeKloud) and **application security** skills (PortSwigger Web Security Academy).

Technical Skills

Cloud & Infrastructure: Microsoft Azure, Azure NSGs, Linux Hardening, ELK Stack

Network & Architecture: TCP/IP, Subnetting, VLAN Segmentation, Inter-VLAN Routing, Firewall Configuration, MQTT

Application Security: REST API Hardening, RBAC, AES Encryption, Secure Auth Pipelines, Audit Logging, GDPR, HIPAA

Programming: Python (Flask), Bash, C/C++, Java, SQL

Certifications: ISC² CC (2025) | CCNA (Cisco)

Experience

IT & Network Security Intern June 2025 – Aug. 2025

State Bank of Pakistan *Karachi, Pakistan*

- Engineered **VLAN segmentation** and **inter-VLAN routing** across enterprise-grade lab environments, enforcing explicit trust boundaries between isolated network tiers in a regulated financial institution.
- Designed multi-zone **DMZ topologies** in **Cisco Packet Tracer**, modeling controlled ingress/egress flows and reducing lateral movement surface across perimeter segments.
- Configured **stateful firewall** rule sets governing cross-zone traffic; contributed to **ISO/IEC 27001 ISMS** Annex A control documentation for critical banking infrastructure.

Software Engineering Intern (Security-Focused) May 2025 – June 2025

DETA-GEN Genetic Diagnostic Center *Kayseri, Türkiye*

- Hardened healthcare **REST APIs** with **AES encryption** (at-rest and in-transit) and **RBAC authorization** layers, achieving **GDPR** and **HIPAA compliance** across sensitive medical data pipelines.
- Implemented a **secure authentication pipeline** with structured **audit logging**, producing non-repudiable access trails and enforcing **least-privilege** through granular session validation.

Projects

Cloud-Native Deception Architecture | *Microsoft Azure, Python (Flask), ELK Stack, Linux*

- Architected an isolated **honeypot environment** on **Azure** end-to-end: **NSG-enforced** network boundaries, hardened **Linux** compute, and a **Flask** financial API decoy engineered to convert attacker interactions into structured **behavioral telemetry**.
- Built centralized **log aggregation** and visualization on **Elastic Stack (ELK)**, enabling real-time pattern analysis of adversarial methodology across all deception nodes.

AirPass – Multi-Factor Edge Access Control | *Raspberry Pi, Arduino, RFID, Biometrics*

- Designed a split-brain physical security system isolating a **Raspberry Pi** policy engine from an **Arduino** untrusted actuator ,hardware-level **zero-trust** ensuring actuator compromise cannot escalate to the decision plane.
- Implemented a multi-stage authentication pipeline (**RFID** + **biometrics**) enforcing **dual-factor access control** at the edge, with no shared state between the trust domains.

EdgeVision – Distributed IoT Enforcement System | *ESP32, MQTT, Python, State Machines*

- Architected a distributed **MQTT pub/sub** enforcement system across **ESP32** nodes with topic-level access controls isolating sensor data streams from the control plane.
- Built state-machine escalation logic converting raw **edge telemetry** into deterministic enforcement signals , threshold-based behavioral response policies with no manual intervention required.