Muhammad Hassan Raza

BS Information Technology
Quaid-e-Awam University of Engineering, Sciences & Technology
Nawabshah, Sindh, Pakistan

+92 319 3007002
mhassanraza.cloud@gmail.com
mhassanraza.me
github.com/code-with-hassanraza
linkedin.com/in/muhammad-hassan-raza

Objective

Cloud Security Professional-in-Training With Two Remote Internships, 3 Production AWS Security Projects, and 4 Credly-Verified GCP Skill Badges. Built Automated Threat Response System (GuardDuty + Lambda) That Isolates Compromised EC2 Instances Within 5 Seconds. Resolved Live Credential Exposure Incident Using Proper IR Procedures. Pursuing CompTIA Security+ (Sep 2026) and AWS Solutions Architect Associate (Jan 2027) on a 24-Month Roadmap Targeting AWS Security Specialty SCS-C02 by Sep 2027.

Experience

•Cloud Computing Intern (AWS/Azure) @DecodeLabs | Student ID: CC06261176 *May 2026 – Jun 2026*
Remote

- Deployed Production Static Site on **AWS S3** + **CloudFront** with SSL/TLS Encryption, Custom S3 Bucket Policy, and CachingOptimized CDN Distribution.
- Architected **Private-Subnet RDS MySQL** (Not Publicly Accessible) with SSH Tunnel via EC2 Bastion Host; Built Python Script (PyMySQL + SSHtunnel) for Secure Programmatic DB Access.
- Detected and Resolved **Security Incident SEC-2026-001** (GitGuardian Alert) – Hardcoded RDS Credentials Exposed in a Public Repo; Revoked, Rotated, and Fully Remediated Within 2.5 Hours With a Documented Incident Report.

•Cyber Security Intern @Arch Technologies, Islamabad | Intern ID: ARCH-2610-0558 *Jan 2026 – Feb 2026*
Remote

- Built a Python + Scapy **Network Packet Sniffer** to Capture and Classify Live TCP/UDP/ICMP Traffic Using Npcap for Windows-Level Raw Packet Capture.
- Developed an **Educational Keylogger** to Study Keystroke-Based Attack Vectors and Document Defensive Countermeasures.
- Conducted **Digital Forensics** with Recuva; Documented Data-Overwrite Behavior and File-Recovery Limitations of Forensic Tools.
- Trained an **ML Fraud Detection Model** on 284,807 Transactions (99.9% Accuracy); Optimized Recall for Imbalanced Datasets Using Pandas and Scikit-learn.

Projects

•The Secret Keeper — Automated Secrets Management & Encryption *Aug 2026*
AWS KMS, Secrets Manager, Lambda, VPC Interface Endpoints, CloudTrail

- Migrated Database Credentials and S3 Encryption From SSE-S3 to KMS-Backed Envelope Encryption (SSE-KMS), Verified via CloudTrail GenerateDataKey Audit Logging.
- Automated 30-Day Secrets Rotation for RDS Credentials Using a VPC-Deployed Lambda Function, Resolving Private Connectivity via a VPC Interface Endpoint for Secrets Manager.
- Eliminated Static, Long-Lived Database Credentials by Migrating to AWS Secrets Manager With Customer-Managed KMS Key (CMK) Encryption.

•The Watchman — Automated AWS Threat Detection & EC2 Isolation *Jul 2026*
GuardDuty, EventBridge, Lambda (Python 3.12), Security Hub, boto3

- Engineered Automated Incident Response Pipeline Using Amazon GuardDuty, EventBridge, and Lambda That Detects HIGH/CRITICAL Severity Threats With Zero Human Intervention Required.
- Automated EC2 Instance Isolation Within **5 Seconds** of Threat Detection by Programmatically Replacing All Security Groups With a DENY-ALL Policy.
- Configured Security Hub With CIS AWS Foundations Benchmark (170+ Controls) and Integrated Real-Time Slack Alerting for Continuous Compliance Monitoring.

•The Data Warehouse — Private Cloud Database Architecture *Jun 2026*
AWS RDS MySQL, EC2, VPC, Security Groups, Python (PyMySQL, sshtunnel)

- Architected Zero-Public-Exposure RDS MySQL Deployment Inside a Private VPC Subnet, Routing All Database Traffic Through an EC2 Bastion Host via Encrypted SSH Tunneling.
- Enforced Least-Privilege Security Group Rules: RDS Accepts Connections Only From the Bastion Host's Security Group Reference, Eliminating IP-Based Access Controls Entirely.
- Developed Python Database Client Using sshtunnel and PyMySQL; Resolved paramiko Version Compatibility Conflicts Affecting Production Tunnel Stability.

Technical Skills

Cloud Security (AWS & GCP): IAM, VPC Networking, Security Groups, Private Subnets, S3 Bucket Policies, SSL/TLS, EC2, RDS, Lambda, CloudFront, CloudWatch, GuardDuty, Security Hub, Secrets Manager, KMS, EventBridge, CloudTrail, SSH Tunneling, Least-Privilege Access, CIS AWS Foundations Benchmark, Cloud Security Fundamentals, GKE (Kubernetes), App Engine, Cloud Build, DevOps Workflows, Compute Engine.
Cybersecurity: Packet Analysis (TCP/UDP/ICMP), Digital Forensics, Fraud Detection (ML), Incident Response (Manual & Automated), Threat Detection, Credential Management, Firewall Rules, SSH Key Authentication.
Programming & Tools: Python (Scapy, Pandas, Scikit-learn, PyMySQL, SSHtunnel, boto3), SQL/MySQL, C/C++, Bash/Shell, HTML5, CSS3, Git, GitHub, AWS CLI, VS Code, Nginx, Npcap, Linux (Amazon Linux 2023).

Education

- **BS Information Technology** *2024 – Present (Expected 2028)*
  Quaid-e-Awam University of Engineering, Sciences & Technology, Nawabshah
- **Diploma in Information Technology (DIT)** *Sep 2023 – Aug 2024*
  Lal Computer Institute, Nawabshah | Affiliated: SBTE Karachi (Reg: 005-2023-72171-02) Grade: A | 1380 / 1800

Certifications & Credentials

- **GCP Skill Badges ×4 (Credly Verified)** – Cloud Security Fundamentals, Cloud Network, DevOps, Kubernetes
- **Cyber Security Internship & Training Program** – Arch Technologies, Islamabad | ID: ARCH-2610-0558 *Feb 2026*
- **Cloud Computing Industrial Training (AWS/Azure)** – DecodeLabs | Student ID: CC06261176 *Jun 2026*
- **Diploma in Information Technology (DIT)** | **Grade: A** – Lal Computer Institute, Nawabshah | SBTE Karachi *Aug 2024*