AARJAN POKHAREL

workwithaarjan@outlook.com | (937) 903-3799 | Fairborn, OH 45324 | LinkedIn | GitHub | Portfolio Website

PROFESSIONAL SUMMARY

AWS Certified Solutions Architect Associate, who designs secure, fault-tolerant cloud infrastructure and owns the architecture and risk tradeoffs behind it, isolating workloads, enforcing least privilege, and building repeatable, automated deployments. Backed by two years of professional security experience leading vulnerability assessments, penetration testing, and ISO 27001 audits for banking and financial clients, with hands-on depth across AWS, Terraform, containers, CI/CD, and Linux.

TECHNICAL SKILLS

Cloud & Infrastructure: AWS (EC2, VPC, S3, RDS, ECR, IAM, CloudWatch, CloudFormation), Azure, GCP, Infrastructure as Code, Cloud Migrations
DevOps & Automation: Docker, Docker Compose, Kubernetes, Terraform, CI/CD, GitHub Actions, Jenkins, Ansible, GitLab
Linux & Systems: Linux Administration (RedHat, Ubuntu, Amazon Linux), Windows Server, Shell Scripting, System Monitoring, Troubleshooting
Databases: MySQL, PostgreSQL, MSSQL, NoSQL, Data Warehousing
Networking: TCP/IP, DNS, Routing, Firewalls, Load Balancers, VPN, Network Security
Security: IAM, Vulnerability Management, Penetration Testing, Compliance Frameworks (ISO 27001), Security Best Practices, OAuth2, JWT
Programming & Scripting: Python, Django, FastAPI, Bash, SQL, Java, JavaScript, React, Nextjs, C#, .Net, Visual Studio, Go (learning), Configuration management automation
Tools & Monitoring: Git, GitHub, CloudWatch, Grafana, Wireshark, Nmap, REST APIs, GraphQL, Apache Kafka, RabbitMQ, SQS/SNS

CERTIFICATIONS

AWS Certified Solutions Architect Associate (SAA-CO3) - Verify on Credly

PROJECTS

Cloud-Native Portfolio Web Application (AWS) **GitHub**

- Architected a full-stack app (Next.js / Django REST / PostgreSQL) as isolated containerized services so a fault or compromise in one tier could not cascade to the others; orchestrated with Docker Compose for reproducible builds.
- Placed a single hardened entry point; Nginx reverse proxy terminating TLS, via Let's Encrypt in front of all services rather than exposing application ports directly, shrinking the public attack surface.
- Reduced exposure further by keeping internal ports off the public network, relocating the admin interface off its default path, and enforcing CSRF/proxy-trust rules correct for TLS termination.

CI/CD Pipeline for Dockerized API Application (AWS) **GitHub**

- Provisioned the entire AWS environment (VPC, subnets, routing, security groups, IAM, EC2) as code with Terraform so infrastructure was version-controlled, auditable, and reproducible rather than hand-built and undocumented.
- Automated build-and-deploy of a containerized Flask API via GitHub Actions and Amazon ECR, removing manual deployment as a source of human error and inconsistent releases.
- Scoped IAM roles to least privilege and tightened security groups to keep a compromised component's blast radius minimal.

Secure 3-Tier AWS Architecture with Automated Deployment **GitHub**

- Architected a multi-AZ 3-tier design so a single-AZ failure cannot take the service down, placing the RDS MySQL database in private subnets so it stays unreachable from the internet even if the web tier is breached.
- Chose a NAT Gateway for controlled outbound access while holding inbound exposure at zero, a deliberate security-over-cost tradeoff, and enforced tier-to-tier security group rules to contain lateral movement.
- Codified the full design in Terraform and GitHub Actions for repeatable, reviewable, version-controlled deployments.

Multi-Container Microservices App with Docker Compose **GitHub**

- Separated API and databases into independent containerized microservices to isolate failure domains and let each scale and be patched independently. Also, diagnosed container-networking issues and tuned for reliable service-to-service communication.

Private EC2 to S3 Access via VPC Gateway Endpoint **GitHub**

- Designed private S3 access for isolated EC2 instances via a VPC Gateway Endpoint so data never crossed the public internet, layering IAM roles and bucket policies for defense in depth; gated SSH through a single bastion host as one controlled entry point, all provisioned in Terraform.

PROFESSIONAL EXPERIENCE

Information Security Engineer - Biz Serve IT Pvt. Ltd. **June 2023 – Dec 2024**

- Led teams of 5–7 engineers across 8 security audit engagements for banking, microfinance, IT, and insurance clients, owning delivery to 100% ISO 27001 conformance and cybersecurity best practices.
- Reviewed and hardened Linux/Windows server, firewall, and network configurations across 90+ assets in 20+ organizations, prioritizing remediation by real-world exploitability and business impact so the most dangerous vulnerabilities were resolved first within tight client downtime limits
- Ran vulnerability assessments and penetration tests across networks, databases, and applications, translating findings into prioritized remediation; served as primary client contact across 9 engagements, communicating risk to both technical teams and decision-makers.

Cybersecurity Analyst Intern - Reanda Biz Serve Pvt. Ltd. **Feb 2023 – May 2023**

- Identified and documented critical endpoint vulnerabilities, framing each finding by its impact so the development team could prioritize fixes.
- Validated web assets and configurations using Linux-based security tooling and established frameworks, producing remediation reports from results that guided developers to the right fixes.

EDUCATION

M.S. Computer Science - Wright State University, Dayton, OH **Expected Aug 2027**
Relevant Coursework: Advanced Cloud Computing, Distributed Computing, Cyber Network Security, Advanced Software Engineering, Artificial Intelligence of Things

B.S. Computer Science & Information Technology - Tribhuvan University, Nepal **Dec 2023**
Relevant Coursework: Cloud Computing, Computer Networks, Software Engineering. Data Warehousing & Mining, Artificial Intelligence