Shadab Akram

Riyadh, Saudi Arabia | +966 573280188 | shadab.akram@gmail.com

LinkedIn: linkedin.com/in/shadab-akram | **Portfolio:** www.shadabakram.com

Senior DevOps & Cloud Security Engineer with **8+** years designing, implementing, securing, and automating enterprise solutions across **AWS**, **GCP**, and **Azure**. Multiple architect-level certifications with proven ability to deliver cost-effective, compliant, and secure high-performing cloud platforms.

SUMMARY

- **8+** years of experience designing, implementing, securing, and operating large-scale platforms on **AWS**, **GCP**, and **Azure** for banking, and enterprise clients.
- **13+** architect-level certifications (**AWS**, **GCP**, **Azure**, **Kubernetes**, **Terraform, Cloud Security**), enabling end-to-end ownership from architecture to implementation and operations.
- Built and operated Kubernetes platforms (**EKS**/**GKE**/**AKS**) using **Terraform**/**Ansible** and **GitOps** (**Argo CD**), **Docker** and **Helm**. supporting highly available microservices and frequent releases.
- DevSecOps Lead **shift-left CI/CD security** (SAST/DAST/SCA) and **IaC security** (policy-as-code).
- Certified Cloud Security expert (**AWS Security Specialty**, **GCP Security** Engineer, **Azure Security).**
- Implemented and managed CSPM, CNAPP, and SIEM solutions to enforce compliance (HIPAA, PCI DSS, NIST, CIS) via Prisma Cloud plus native cloud security services.
- Cloud security architecture across **IAM** (**least privilege**/**RBAC**), network segmentation, encryption in transit/at rest**,** secrets management, vulnerability management and continuous threat detection.
- Defined **SLIs**/**SLOs**/**SLA**, **error budgets**, **on-call**, **alert tuning**, **incident management**, **postmortems/RCA**, **capacity planning**, and **reliability automation** to improve **uptime and MTTR**.
- Expert at building real-time monitoring/alerting (**Prometheus**, **Grafana**, **Loki**, **Dynatrace**, **AppDynamics**, **ELK**) and leading incident response with thorough RCA playbooks.
- Backend Developer with hands-on experience in designing and developing scalable microservices and **REST APIs** using **Java Spring Boot** and **Go**, with additional scripting capabilities in **Python**.

CERTIFICATIONS

- AWS Certified Solutions Architect – Associate (**SAA-C03**) — AWS — Credential URL/ID
- AWS Certified Solutions Architect – Professional (**SAP-C02**) — AWS — Credential URL/ID
- AWS Certified DevOps Engineer – Professional (**DOP-C02**) — AWS — Credential URL/ID
- AWS Certified Security – Specialty (**SCS-C02**) — AWS — Credential URL/ID
- AWS Certified Machine Learning – Specialty (**MLS-C01**) — AWS — Credential URL/ID
- Professional Cloud Architect — Google Cloud — Credential URL/ID
- Professional Cloud Security Engineer — Google Cloud — Credential URL/ID
- Microsoft Certified: Azure Administrator Associate (**AZ-104**) — Microsoft — Credential URL/ID
- Microsoft Certified: Azure Solutions Architect Expert (**AZ-305**) — Microsoft — Credential URL/ID
- Microsoft Certified: Azure Security Engineer Associate (**AZ-500**) — Microsoft — Credential URL/ID
- Certified Kubernetes Application Developer (**CKAD**) — CNCF — Credential URL/ID
- Certified Kubernetes Administrator (**CKA**) — CNCF — Credential URL/ID
- HashiCorp Certified: Terraform Associate (**003**) — HashiCorp — Credential URL/ID
- Verification: https://www.linkedin.com/in/shadab-akram/ (Licenses & Certifications)

TECHNICAL SKILLS

- **Cloud platforms:** Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure
- **AWS:** VPC, EC2, EKS, ECS, ALB/NLB/ELB, RDS, S3, EFS, SNS, SQS, IAM, CloudWatch, CloudTrail, Config, KMS, WAF, GuardDuty, Shield, Macie, Inspector, CodeCommit, CodeBuild, CodePipeline, Organizations, Control Tower
- **GCP:** Compute Engine (GCE), GKE, VPC, Cloud Storage, BigQuery, Artifact Registry (GCR legacy), Cloud Monitoring and Cloud Logging (Stackdriver), IAM, Cloud KMS, Security Command Center, Cloud Armor, Secret Manager
- **Azure:** VMs, AKS, ACR, VNets, Load Balancer/App Gateway, Entra ID (Azure AD), Azure Monitor, Defender for Cloud, DDoS Protection, WAF, Azure DevOps, Azure Policy, Key Vault
- **Containers and orchestration:** Docker, Kubernetes (EKS/GKE/AKS), Helm, GitOps (Argo CD)

- **CI/CD and release:** Jenkins, GitLab CI, Argo CD, Spinnaker; blue-green, canary
- **Infrastructure as Code:** Terraform, AWS CloudFormation, Ansible
- **Observability and SRE:** Prometheus, Grafana, Loki, Promtail, CloudWatch, Dynatrace, AppDynamics, SLI/SLO, alerting, incident response, capacity planning, error budgets, toil reduction, chaos engineering, performance engineering
- **Security and compliance:** Prisma Cloud, Trivy, SonarQube, OWASP ZAP, Burp Suite, Splunk, Veracode, Checkmarx, OPA, Sentinel, HashiCorp Vault, KMS (AWS/GCP/Azure), CNAPP, CSPM, CWPP, Zero Trust Architecture, Shift-Left Security, CIS Benchmarks, AWS Security Hub, Microsoft Defender for Cloud, HIPAA, HITRUST, PCI DSS, SOX, NIST, CIS, IAM federation (SSO), MFA, least privilege, privileged access management (PAM), key rotation, encryption in transit/at rest, secrets management, security guardrails, continuous compliance, security automation, incident response, threat investigation, Pod Security Standards/Admission, NetworkPolicies, OPA Gatekeeper
- **Programming and scripting:** Java (Spring Boot), Python, Go, Bash, YAML, JSON
- **Web and app servers:** Apache HTTP Server, Tomcat, WebLogic
- **Databases:** Oracle 11g, MySQL, PostgreSQL
- **Networking + OS Security:** Linux, TCP/IP, DNS, TLS, firewalls, VPNs
- **Others technologies:** HTML5, CSS, JavaScript, TypeScript, JSON, XML, HTTP, Node.js, Next.js, React, Nexus, JFrog

PROJECTS/ASSIGNMENTS

Wipro — Senior DevOps & Cloud Security Engineer | Mar 2023 - Present
Client: Standard Bank (South Africa)
Responsibilities:
- Designed and implemented secure, highly available cloud architectures across AWS, Azure, and GCP, aligning with enterprise security baselines and audit requirements.
- Automated infrastructure provisioning with Terraform and Ansible, reducing manual provisioning effort, eliminating configuration drift, and enabling consistent environments across dev to prod.
- Drove cloud cost optimization by rightsizing instances, eliminating underutilized resources, and leveraging storage and reservation strategies, improving cost efficiency while meeting SLOs.
- Containerized legacy applications with Docker and migrated them to Kubernetes (EKS/GKE/AKS), improving scalability and standardizing deployment patterns across multiple regions and clouds.
- Implemented CSPM across AWS Security Hub, GCP Security Command Center for Cloud to continuously detect misconfigurations and enforce organizational security and compliance.
- Strengthened cloud identity security with IAM least privilege, role-based access, and periodic access reviews; reduced standing privileges where possible.
- Designed and maintained end-to-end CI/CD pipelines (Jenkins, Argo CD) with automated testing, scanning, and approval workflows, shortening release cycles and improving deployment reliability.
- Managed identity and access management (IAM) across cloud environments, implementing the principle of least privilege and role-based access control (RBAC) for users and services.
- Established centralized observability stack using Prometheus, Grafana, Loki, and CloudWatch; built actionable dashboards and alerts that enabled faster detection and diagnosis of performance and availability issues.
- Improved Kubernetes security posture through RBAC hardening and cluster controls (e.g., Pod Security standards / admission policies) aligned to CIS benchmarks.
- Integrated robust security controls into cloud architectures by embedding industry-specific compliance standards such as HIPAA, GDPR, ISO 27001, PCI DSS, NIST, and CIS to mitigate vulnerabilities and protect critical data.
- Embedded shift-left security into delivery pipelines via SonarQube Quality Gates, SAST/DAST (Checkmarx/Veracode/OWASP ZAP), and container scanning (Trivy/Prisma) with fail-fast policies, preventing vulnerable builds from reaching production.

Wipro — DevSecOps/SRE Engineer| Mar 2021 – Mar 2023
Client: Mastercard (USA)
Responsibilities:
- Integrated SAST, DAST, and SCA tools (Checkmarx, SonarQube) into CI/CD pipelines, shifting security left and reducing vulnerability discovery in production by enforcing quality and security gates.

- Automated infrastructure creation using Terraform and configuration management via Ansible, significantly decreasing manual changes and increasing repeatability and auditability of infrastructure changes.
- Conducted regular security audits, vulnerability assessments, and continuous risk assessments through proactive threat modeling, ensuring robust cloud security posture and compliance with industry standards.
- Implemented security automation for misconfiguration detection and remediation using policy-as-code and pipeline enforcement.
- Designed and implemented HA and DR architectures with clear RPO/RTO objectives and controlled rollout strategies (blue-green, canary), supporting 99.99% availability for payment-critical services.
- Introduced SLIs/SLOs and tuned alerting policies, reducing alert noise and cutting MTTR from 45 minutes to 18 minutes for high-severity incidents through better detection, routing, and playbooks.
- Enforced secure infrastructure via IaC scanning (Terraform/CloudFormation) and policy-as-code (OPA, Sentinel), preventing non-compliant resources from being deployed.
- Developed Groovy, Shell, and Python tooling to auto-remediate common pipeline issues, enforce branching and naming conventions, and reduce repetitive toil for engineers.
- Set up centralized logging and security monitoring using CloudTrail, Azure Monitor, Stackdriver, and SIEM integrations, improving traceability and enabling faster security investigations.
- Embedded OWASP Top 10 checks and **secure** SDLC practices into CI/CD pipelines, ensuring application changes were threat-modeled, code-reviewed and scanned before reaching production.

NOUS Infosystem — DevOps/DevSecOps Engineer | Jan 2019 – Feb 2021
Client: GE (General Electric USA)
Responsibilities:
- Designed and operated AKS-based platforms and automated delivery workflows with Spinnaker and Jenkins, enabling consistent, repeatable deployments to multiple environments.
- Built tooling in Go to extend AKS capabilities, including namespace/pod-level billing visibility, helping product teams understand and optimize their cloud spend.
- Implemented container monitoring with Prometheus and Grafana, defining key metrics and alerts that improved visibility into application performance and resource usage.
- Provisioned GCP dev/stage/prod environments with Terraform and shipped services to GKE, securing them with Cloud IAM, Security Command Center, VPC Service Controls, and Cloud Monitoring/Logging.
- Automated infrastructure workflows using Terraform + Ansible + shell scripts, reducing manual change time by 40% and mitigating configuration drift between environments.
- Remediated critical security findings surfaced by Security Hub/SCC/Defender/Prisma Cloud and enforced CIS Benchmark-aligned policies via OPA/Sentinel pre-merge checks, strengthening the security posture.
- Implemented SSO and MFA for engineering users, and standardized application authentication using OAuth2/OIDC, strengthening identity security while keeping developer experience smooth.

Cotelligent — Java Developer | Feb 2017 - Nov 2017
Client: IBM (Bangalore, IN)
Responsibilities:
- Developed and maintained backend services in Java/Spring Boot with JPA and PostgreSQL, focusing on clean, testable code and stable APIs
- Implemented automated tests (JUnit, Selenium, REST Assured) to improve deployment quality and catch regressions early in the pipeline.
- Built and maintained reusable JavaScript/TypeScript UI libraries and state management solutions, enhancing code maintainability, developer productivity, and user experience.
- Developed dynamic, server-side rendered applications with Next.js and React.js, leveraging TypeScript for type-safe components, optimized performance, and improved SEO.

ACADEMIC QUALIFICATION

- Master of Computer Applications (MCA), Computer Science — Sikkim Manipal University (SMU), 2012