

MUHAMMAD SALAHUDDIN

Senior DevOps Engineer | AWS & Cloud Infrastructure & DevSecOps

+92 333 6074999 | salahuddin76@hotmail.com | [linkedin.com/in/muhammad-salahuddin](https://www.linkedin.com/in/muhammad-salahuddin)

PROFESSIONAL SUMMARY

Senior DevOps Engineer with 8+ years designing, securing, and operating cloud-native infrastructure across AWS, Azure, and GCP for fintech, SaaS, e-commerce, and AI-driven platforms. Deep hands-on expertise in Kubernetes (EKS/AKS/GKE), Terraform-driven infrastructure as code, and end-to-end CI/CD pipeline design with Jenkins, GitHub Actions, AWS CodePipeline, and ArgoCD. Strong DevSecOps focus — integrating SIEM, vulnerability management, penetration-testing workflows, and secrets management into pipelines aligned with PCI-DSS, SOC2, and HIPAA. Experienced across cloud and on-premises (VMware vSphere/ESXi) environments, building highly available, observable, cost-optimized systems for both monolithic and microservices workloads. Combines hands-on engineering with architecture and consulting, translating business requirements into secure, scalable cloud solutions.

CORE SKILLS & TECHNOLOGIES

Cloud Platforms: AWS (EC2, EKS, ECS, Fargate, Lambda, S3, RDS/Aurora, VPC, Transit Gateway, IAM, CloudFront, Route 53, CloudWatch, SQS, SNS, Secrets Manager, SES, API Gateway, CodeBuild, CodeDeploy, CodePipeline, ECR, ElastiCache), Azure (VMs, AKS, App Service, Azure DevOps, Azure AD, Blob Storage, Key Vault), GCP (GKE, Compute Engine, Cloud Build, Cloud Run, Cloud SQL, Secret Manager, Pub/Sub, IAM)

Containers & Orchestration: Docker, Kubernetes (EKS, AKS, GKE), OpenShift, Helm, KEDA (event-driven autoscaling), Cluster Autoscaler, Secrets Store CSI Driver

Infrastructure as Code & Config Mgmt: Terraform, AWS CloudFormation, Ansible

CI/CD & GitOps: Jenkins, GitHub Actions, GitLab CI, AWS CodePipeline, ArgoCD — pipeline design & architecture, GitOps workflows

DevSecOps & Security: SIEM, penetration testing, vulnerability management, SonarQube, Snyk, OWASP ZAP, IAM least-privilege design, secrets management & credential rotation, PCI-DSS / SOC2 / HIPAA

Observability & Monitoring: Prometheus, Grafana, Amazon CloudWatch, ELK Stack, Datadog, Nagios, Zabbix, AI-based log anomaly detection, SLO/SLI frameworks

Automation & AI Tooling: Python (boto3), Bash, n8n (self-hosted workflow automation), AI/LLM-assisted operations

Networking & Connectivity: VPC & subnet design, Transit Gateway, OpenVPN, WireGuard, Tailscale, AWS Client VPN, CDN (CloudFront), pfSense

Databases & Caching: MySQL, MongoDB, PostgreSQL, Amazon RDS/Aurora, ElastiCache / Valkey, Redis

Virtualization & On-Prem: VMware vSphere / ESXi, Linux server administration (RHEL, CentOS, Ubuntu, Amazon Linux), Windows Server

App Stack & Version Control: Java, Node.js, Python, PHP; GitHub, GitLab, Bitbucket

PROFESSIONAL EXPERIENCE

Team Lead | Senior DevOps Engineer — Rough Copies

Jul 2024 – Present

Led a DevOps team architecting and operating multi-cloud infrastructure (AWS, GCP) across a diverse portfolio of production platforms — fintech SaaS, social media, e-commerce, and AI-driven applications — owning DevOps strategy end-to-end from network design through observability and security.

- Designed and implemented multi-account AWS architecture including VPC topologies, network segmentation, and IAM governance, enabling secure, scalable deployment of services across multiple client environments.
- Architected and maintained containerized platforms on Amazon EKS, ECS, and Google GKE with automated node scaling (Cluster Autoscaler/KEDA) for both monolithic and microservices workloads, standardizing deployment patterns across applications.
- Built and fully managed multi-application AWS infrastructure as code with Terraform — provisioning networking, compute, containers, databases, and IAM end-to-end — with Fun Social, ScoutPro, and Artfully entirely managed through Terraform for repeatable, version-controlled, drift-free deployments.
- Built and operated cloud infrastructure for a range of production products, including AutoLeap (SaaS automotive shop-management platform), Fun Social (Python-based social media application), an AI-based barbershop booking platform (HairCut), an AI-driven pharmacy solution (GCP/Java-based), ScoutPro and The Dust Test (AWS/PHP applications), and HomeGlance (AWS/Node.js).
- Architected a multi-region, highly available deployment for Fun Social, engineering cross-region disaster recovery with automated failover and CloudFront CDN delivery for low-latency global access and resilience against regional outages.
- Standardized Helm-based deployment patterns and GitOps workflows using ArgoCD across platform services, enforcing declarative configuration management and drift detection for consistency across dev, staging, and production.
- Designed and architected CI/CD pipelines using GitHub Actions, AWS CodePipeline, Jenkins, and ArgoCD, implementing GitOps-driven deployment workflows for reliable, repeatable releases.

- Embedded DevSecOps security gates into CI/CD pipelines — static code analysis (SonarQube), dependency and vulnerability scanning (Snyk), container image scanning, and automated testing — blocking insecure or non-compliant builds from reaching production.
- Deployed a self-hosted n8n automation platform on Kubernetes with KEDA-based event-driven autoscaling, enabling workflow automation that scales to zero when idle for cost efficiency.
- Implemented AI-based log anomaly detection to proactively surface abnormal patterns in application and infrastructure logs, improving early detection of issues before customer impact.
- Established DevSecOps practices across the estate — SIEM integration, penetration-testing workflows, and vulnerability management — hardening security posture across client environments.
- Secured a Next.js frontend on EKS by integrating AWS Secrets Manager with the Secrets Store CSI Driver to remove hardcoded credentials, coordinating a Jenkins pipeline in an isolated VPC for build-time secret injection; led a credential rotation response after identifying exposed keys during a security review.
- Built an AWS ECS-based recommendation API integrating SES, ECR, CodeBuild, ElastiCache/Valkey, and Secrets Manager; resolved a CodeBuild pipeline failure caused by incorrect Secrets Manager JSON parsing in the buildspec.
- Drove cost optimization and high-availability initiatives, building resilient ecosystems with full observability (Prometheus, Grafana, CloudWatch) and backup/disaster-recovery strategies across cloud environments.

Team Lead | Principal DevOps Engineer — Systems Limited

Mar 2020 – Jun 2024

Led a DevOps team owning infrastructure architecture, security operations, and platform reliability for EP-Systems, running two production fintech applications (OneLoad, OneZapp) on hybrid AWS and on-premises infrastructure with 24x7x365 availability requirements.

- Architected and designed hybrid cloud and on-premises infrastructure supporting high-transaction Java-based fintech platforms, spanning AWS and on-premises environments in a hybrid architecture.
- Designed and operated a microservices architecture for the fintech applications, containerizing services on Amazon EKS with standardized Helm deployments, service-to-service communication, and independent scaling.
- Ensured reliability of payment and transaction processing for the fintech platforms (OneLoad, OneZapp), owning application availability, capacity planning, and incident response for high-volume financial workloads.
- Led Terraform and CloudFormation infrastructure-as-code initiatives, standardizing provisioning across development, staging, and production and enforcing consistent, compliant baseline configurations.
- Designed and built DevSecOps CI/CD pipelines with Jenkins and GitLab CI, embedding the full secure-delivery lifecycle — static application security testing (SonarQube), dependency and vulnerability scanning (Snyk), container image scanning, automated unit and integration testing, and security gate enforcement — to block insecure or non-compliant builds before promotion to production.
- Delivered Kubernetes container orchestration on Amazon EKS and OpenShift for the fintech applications, designing cluster architecture, node groups, and Helm-based standardized deployment patterns; ran production Java microservices workloads on OpenShift with standardized CI/CD and observability integration.
- Directed SOC operations, vulnerability remediation, and compliance enforcement across PCI-DSS, SOC2, and HIPAA frameworks for a regulated fintech environment.
- Architected monitoring and observability with Prometheus and Grafana across 10+ production environments, with centralized log management via the ELK stack and proactive alerting.
- Implemented IAM least-privilege policies and secrets management, embedding automated compliance checks and vulnerability scanning into delivery workflows.
- Automated configuration management and deployment workflows using Ansible, standardizing provisioning and security patching across environments.
- Owned application availability and incident response for mission-critical fintech services, troubleshooting JBoss, GlassFish, and microservice issues in production and reviewing release notes.
- Designed and managed VPC/subnet architecture with cross-zone connectivity and IP/subnet-level ACL blocking for suspicious traffic; managed CloudFront CDN (server and S3 origins) for performance.
- Drove FinOps and AWS cost optimization — rightsizing instances, tuning resource allocation, and managing AMI/snapshot/volume lifecycle — reducing cloud spend while sustaining 24x7 fintech availability, alongside RDS administration, Route 53 / GoDaddy DNS, and backup/restore across environments.

DevOps Engineer — Wadic Solution

Jul 2019 – Feb 2020

Delivered DevOps and infrastructure support across AWS cloud and on-premises VMware vSphere environments, managing ERP, CRM, and client-facing web applications.

- Deployed and managed Odoo ERP and CRM systems with Nginx on Ubuntu, maintaining service uptime and performance for client operations.
- Deployed, configured, and operated PHP- and Python-based client applications, owning build, deployment, and ongoing operational support across environments.

- Performed Linux server administration across client infrastructure — provisioning, hardening, patching, and performance tuning for production and staging systems.
- Built a centralized monitoring system using Python and Django to track health, uptime, and performance metrics across all client deployments, providing a single pane of visibility for the operations team.
- Configured and managed high-availability database clusters (MySQL InnoDB and MongoDB/NoSQL), implementing replication, failover, and automated backup routines for production data.
- Administered on-premises VMware vSphere/ESXi infrastructure alongside AWS-hosted workloads in a hybrid setup, managing VMs, storage, and resource allocation.
- Built and operated CI/CD pipelines using Jenkins for automated build, test, and deployment, improving release consistency across the engineering team.
- Designed disaster recovery and automated backup procedures with documented recovery runbooks, ensuring availability and data integrity across client environments.
- Provided AWS Connect configuration support per client requirements and hardened Git server security and access control.

Associate DevOps Engineer — AdMaxim Inc.

May 2017 – Jun 2019

Supported infrastructure and DevOps operations for a digital advertising platform, including the Pinpoint solution, administering AWS and Linux/Windows server environments for high-availability production workloads.

- Configured foundational AWS environments — VPC networks, EC2 instance fleets, and security group policies — establishing baseline cloud architecture for hosting the advertising platform and internal applications.
- Administered Linux and Windows server infrastructure, performing OS-level configuration management, system hardening, and patch compliance to keep development and production environments consistent and secure.
- Automated deployment, provisioning, and security patching using Ansible, and built CI/CD workflows with Jenkins to reduce manual operational effort.
- Developed Python and Bash automation for operational workflows — patching pipelines, log collection and centralization, system health reporting, and configuration compliance checks across server infrastructure.
- Implemented monitoring and alerting with Nagios, Zabbix, and AWS CloudWatch — configuring custom metrics, threshold-based alarms, and dashboards for visibility into server, application, and resource health.
- Supported Java-based application stacks backed by MySQL and MongoDB, handling deployment, tuning, and day-to-day operational tasks.
- Built backup and disaster-recovery procedures including automated EBS snapshot policies and S3 cross-region replication, with documented recovery runbooks to strengthen organizational resilience.
- Assisted with IAM user and role reviews, identifying over-permissioned accounts and contributing to least-privilege access policies across AWS resources.
- Integrated OWASP ZAP into the security testing lifecycle for continuous web application vulnerability scanning, and provided cross-functional support to development teams on deployment and environment issues.

EDUCATION

MS, Computer Science — Riphah International University, Lahore

BS, Telecom & Networking — COMSATS Institute of Information Technology, Sahiwal