



# Priyanga Mohan

## Senior Software Engineer – DevOps

+91 93639 45199

priyangam159@gmail.com

Chennai, India.

### KEY SKILLS

- DevOps Strategy & Implementation
- CI/CD Pipeline Development & Automation
- Kubernetes Cluster Management (EKS)
- Docker Containerization & Image Optimization
- Infrastructure as Code (IaC) with Ansible
- Cloud Infrastructure Management (AWS)
- Application Deployment & Release Automation
- Performance Monitoring & Alerting
- Security & Compliance (RBAC, Network Policies, Secrets Management)
- Cross-functional Team Collaboration & Mentoring
- Disaster Recovery & High Availability Planning
- Agile/Scrum Methodology

### TECHNICAL SKILLS

- **Cloud Platforms:** AWS (EC2, S3, VPC, IAM, CloudWatch, CloudFormation, Route 53, ELB, Secrets Manager, EBS, EKS, ECR)
- **CI/CD Tools:** Jenkins, Nexus, SonarQube, Maven.
- **IaC & Configuration Management:** Terraform, Helm, Ansible.
- **Containerization & Orchestration:** Docker, Kubernetes (EKS).
- **Monitoring & Logging:** Prometheus, Grafana, CloudWatch.
- **Security & Compliance:** AWS IAM, Secrets Manager, HashiCorp Vault.
- **Scripting Languages:** Shell scripting.
- **Build & Artifact Management:** Maven, Nexus.
- **Version Control:** GitHub.
- **Servers:** Apache Tomcat.

### PROFILE

DevOps Engineer with 5+ years of experience in cloud infrastructure and automation. Expertise in designing scalable and highly available cloud environments on AWS. Proficient in AWS services including EC2, S3, VPC, IAM, CloudFormation, EKS, ECR, and ELB. Experienced in building and managing CI/CD pipelines using Jenkins, Nexus, and Artifactory. Skilled in Infrastructure as Code (IaC) with Terraform, Helm, and Ansible. Strong knowledge of containerization using Docker and orchestration with Kubernetes (EKS). Hands-on experience with monitoring and logging tools, including Prometheus, Grafana, and CloudWatch. Implemented automated deployments to reduce release cycles and improve operational efficiency. Proficient in scripting with Shell to automate repetitive tasks and system maintenance. Managed secure credentials using AWS Secrets Manager and HashiCorp Vault. Experienced in version control and collaboration using GitHub. Expertise in building and artifact management using Maven, Nexus. Knowledgeable in server management and deployment on Apache Tomcat. Implemented security best practices, access control, and compliance in cloud environments. Strong problem-solving skills with a focus on improving system reliability and scalability.

### PROFESSIONAL EXPERIENCE

#### Senior Software Engineer (DevOps) | Mar 2020 - Sep 2025 Kapital Information Technologies Pvt Ltd, Hyderabad, India.

- Designed, deployed, and managed scalable AWS cloud infrastructure, including EC2, S3, VPC, ELB, EKS, and ECR.
- Implemented Infrastructure as Code (IaC) using Terraform, CloudFormation, and Helm charts to facilitate automated provisioning.
- Developed and maintained continuous integration and continuous deployment (CI/CD) pipelines utilizing Jenkins, with integration of Maven and Nexus for build and artifact management.
- Containerized applications using Docker and orchestrated deployments on Kubernetes (EKS) to ensure high availability.
- Configured monitoring and alerting systems with Prometheus, Grafana, and CloudWatch to effectively track performance metrics.
- Automated repetitive tasks and deployments through Shell scripting and Ansible playbooks.
- Managed secrets and sensitive credentials utilizing AWS Secrets Manager and HashiCorp Vault.
- Ensured security compliance by implementing IAM policies, access controls, and encryption standards.
- Collaborated with development and QA teams to streamline deployment processes and reduce release cycles.
- Diagnosed and resolved infrastructure and application issues to maintain system reliability and uptime.
- Optimized cloud resources for cost efficiency, performance, and scalability.
- Implemented logging solutions and dashboards for proactive system monitoring.
- Conducted code quality and security assessments using SonarQube.
- Automated server patching, backup, and disaster recovery strategies for critical systems.
- Documented infrastructure configurations, pipelines, and operational procedures to facilitate team knowledge transfer.

# EDUCATION

---



## B.E – Electronics & Communication Engineering | 2015

PSNA College of Engineering and Technology, Tamil Nadu, India.

# PROJECTS DETAILS

---

## Cloud Infrastructure Automation on AWS

**Description:** Automated provisioning, configuration, and management of cloud resources to improve scalability, reduce manual effort, and ensure consistent deployment across environments.

**Tech Stack:** AWS EC2, S3, VPC, CloudFormation, IAM, Terraform, CloudWatch

- Designed and deployed highly available AWS infrastructure using CloudFormation and Terraform.
- Configured VPCs, subnets, NAT Gateways, and security groups for secure networking.
- Managed IAM roles and policies to enforce least privilege access.
- Automated EC2 instance provisioning with Ansible playbooks.
- Implemented ELB for load balancing and EBS for persistent storage.
- Configured S3 buckets with encryption and lifecycle policies for storage optimization.
- Monitored infrastructure using CloudWatch and created custom alarms.
- Implemented disaster recovery strategies with automated snapshots and multi-region setup.
- Integrated AWS Secrets Manager for secure credentials management.
- Provided operational support and troubleshooting for cloud resources.

## CI/CD Pipeline Implementation

**Description:** Implemented automated CI/CD pipelines to streamline application build, test, and deployment processes, improving release efficiency and reducing manual errors.

**Tech Stack:** Jenkins, Git, GitHub, AWS DevOps, Docker, Kubernetes, Maven.

- Developed end-to-end Jenkins pipelines for build, test, and deployment.
- Integrated Maven, Nexus for artifact management.
- Automated code quality checks using SonarQube.
- Configured multi-branch pipeline strategies for feature deployments.
- Implemented rollback mechanisms for failed deployments.
- Automated deployment to EC2 instances and Kubernetes clusters.
- Used GitHub webhooks to trigger pipelines on code commits.
- Managed environment-specific configurations using Helm charts.
- Reduced deployment time by 40% through pipeline optimization.
- Provided pipeline documentation and knowledge transfer to the team.

## Containerization and Orchestration

**Description:** Experience in deploying, managing, and scaling containerized applications in enterprise environments using container orchestration tools for high availability and efficient resource utilization.

**Tech Stack:** Docker, Kubernetes, Elastic Kubernetes Service (EKS), Helm, YAML, CI/CD pipelines.

- Containerized legacy applications using Docker.
- Deployed and managed Kubernetes clusters on EKS.
- Automated Helm chart creation and release management.
- Configured Kubernetes deployments, services, and ingress controllers.
- Implemented CI/CD integration for containerized applications.
- Monitored cluster health using Prometheus and Grafana dashboards.
- Implemented horizontal pod autoscaling for performance optimization.
- Managed container registries with ECR and DockerHub.
- Ensured secure communication between pods using NetworkPolicies.
- Performed regular updates and patching for Kubernetes clusters.

Monitoring and Logging Setup

**Description:** Implemented enterprise-wide monitoring and logging solutions to track server and network performance, detect issues proactively, and automate alerting for faster incident resolution.

**Tech Stack:** AWS CloudWatch, Prometheus, Grafana.

- Implemented centralized logging with CloudWatch Logs and Grafana.
- Configured Prometheus for metric collection and alerting.
- Developed dashboards for system performance and application metrics.
- Automated alert notifications using SNS and Slack integration.
- Conducted root cause analysis for system downtime and performance issues.
- Monitored CPU, memory, and disk usage across servers and containers.
- Established logging standards for all microservices.
- Set up CloudWatch alarms for EC2, ELB, and RDS resources.
- Generated regular performance reports for management review.
- Improved system observability and reduced incident resolution time by 30%.

Security & Compliance Automation

**Description:** Automated security monitoring, compliance checks, and policy enforcement across enterprise servers to ensure secure and compliant IT operations.

**Tech Stack:** AWS IAM, AWS Config,AWS Secrets Manager, HashiCorp Vault, Terraform, Ansible.

- Managed IAM roles and policies to enforce least privilege access.
- Integrated HashiCorp Vault and AWS Secrets Manager for secrets management.
- Automated SSL/TLS certificate management and rotation.
- Implemented infrastructure security best practices using Terraform.
- Conducted periodic security audits and compliance checks.
- Configured security groups and NACLs to restrict access.
- Enforced multi-factor authentication for critical accounts.
- Automated patching of EC2 instances using Ansible.
- Maintained audit logs and compliance documentation for AWS resources.
- Collaborated with security teams to resolve vulnerabilities proactively.

PERSONAL DETAILS

---

Nationality : Indian  
Gender : Female  
Languages Known : English & Tamil

DECLARATION

---

I hereby declare that the information provided above is true and correct to the best of my knowledge and belief.