Zeal Patel

Chicago, IL | 818-914-1343 | zeal.amrish@gmail.com | LinkedIn | Portfolio

EDUCATION

Illinois Institute of Technology, Chicago - IL — Aug 2023 – May 2025
Master's in Computer Science (**GPA 3.8 / 4.0**)

CERTIFICATION

AWS Certified DevOps Engineer – Professional (Verification) — Mar 2025 – Mar 2028
Microsoft Certified: Azure AI Engineer Associate — In Process

SKILLS

- **Programming & Automation:** Python, Bash, Java, C++, JavaScript
- **SRE & DevOps:** AWS (EC2, EKS, Lambda, S3, IAM, VPC), GCP (GKE, IAM, Cloud Functions), Terraform, Ansible, Argo CD, Jenkins, GitHub Actions, Azure DevOps, Docker, Kubernetes
- **Monitoring, Security & Databases:** CloudWatch, Splunk, Datadog, Grafana, Prometheus, ELK, IAM, Guard Duty, HashiCorp Vault, MongoDB, MySQL, SQL

EXPERIENCE

Drevol LLC – Software Engineer Intern (Redmond, WA – Remote) — Aug 2024 – Dec 2024

- Developed scalable microservices on AWS using Python and RESTful APIs, integrating with AWS Lambda, S3, and API Gateway to meet secure and cost-efficient application needs.
- Supported infrastructure automation efforts by writing Infrastructure as Code (IaC) scripts using Terraform and managing deployments through GitHub Actions. Collaborated with DevOps teams to build and troubleshoot CI/CD pipelines, enhancing deployment reliability across staging and production environments.
- Participated in system performance monitoring using DataDog and CloudWatch, contributing to resolution of latency issues and documenting root cause analyses.

ColoXchange NV Inc. – DevOps Engineer Intern (Las Vegas, NV – Remote) — May 2024 – Aug 2024

- Framed and deployed infrastructure on AWS and Azure using Terraform and CloudFormation, reducing setup time by 40% and increasing reliability.
- Orchestrated containerized applications using Docker and Kubernetes (EKS/AKS), supporting zero-downtime updates and maintaining 99.9% uptime.
- Set up monitoring with Prometheus, CloudWatch, and Datadog, which reduced incident response time by 30%. Partnered with QA, development, and product teams to integrate automation into sprint workflows, tripling monthly release volume.

Vishag Tech Pvt Ltd – Site Reliability Engineer (Gujarat, IN- Hybrid) — Mar 2020 – May 2023

- Managed multi-cloud infrastructure across AWS, Azure, and GCP, tuning compute, storage, and network parameters to reduce operational costs by 25%. Wrote automation scripts to manage configuration, access policies, and deployment routines using Python, Bash, and Ansible.
- Responded to outages and performance issues, documented root causes, and added monitoring tools like Prometheus and Grafana to catch future problems early.
- Established secrets management using AWS Secrets Manager, Azure Key Vault, and Hashi Corp Vault to secure credentials and API keys across all environments. Modified IAM roles, S3 policies, and encryption settings using KMS to meet 100% of internal audit requirements.

PROJECT

Cloud-Based Anomaly Detection System using AI

- Designed an anomaly detection pipeline with AWS Lambda, S3, and SageMaker to process infrastructure logs and flag performance issues.
- Trained an LSTM model on historical metrics to detect latency spikes and CPU/memory irregularities with 92% precision. Launched alerts through SNS and integrated with CloudWatch, cutting incident detection time by 40% and enabling automated scaling in production.

Azure VM Deployment Automation

- Created scripts to generate and upload VHD images to Azure, reducing manual provisioning time by 30%. Built a deployment script to launch multiple VMs simultaneously, increasing provisioning speed by 50%.
- Linked the Geneva Monitoring Agent with an AI-based telemetry analysis tool to identify trends and predict failures in real time, improving operational efficiency by 40%.

Security Threat Detection System

- Constructed a real-time system to monitor network traffic using Python, Suricata, and Zeek, reducing security incidents by 30% in the first quarter. Incorporated with ELK Stack for log analysis and alerting.
- Refined detection rules and thresholds through testing and data review, achieving 90% accuracy in identifying and flagging potential threats.