Abhishek Kumar Singh

Senior Site Reliability Engineer & DevOps | Cloud Operations

abhishek.techie21@gmail.com

+91-7411300272

Bengaluru, India

linkedin.com/in/abhishek-techie21

github.com/abhishektechie21-Ops

Education

Bachelor of Technology (B.Tech) in Electronics, *Ideal Institute of Technology*
08/2014 – 07/2018 | Ghaziabad
Percentage: 73%

Engineering Initiatives

- Designed and built a **web-based Terraform dashboard** integrated with an **AI chatbot** assistant to streamline infrastructure provisioning and improve user experience.
- Open-source LLMs (LLaMA) for internal SRE knowledge assistance and RCA exploration.
- Led POC for **SLK Direct** to accelerate SRE journey: aggregated data from **Dynatrace** & **ServiceNow**, built unified ops views and workflows.
- Integrated **AWX** for **event automation** and self-service ops; reduced manual interventions across incident & change processes.
- Built POCs with **Harness** (CI/CD), showcasing automated build/deploy, progressive delivery, and policy checks.
- Evaluated **Nagios, Thousand Eyes, New Relic** for infra/network/app performance; produced comparative findings and adoption recommendations.

Profile

DevOps/SRE Engineer with 7+ years of experience in managing and optimizing cloud operations across **AWS, Azure, and GCP**. Skilled in **Infrastructure as Code (Terraform, Ansible)**, **container orchestration (Kubernetes)**, **Build & Release** and **cloud monitoring/alerting**, ensuring reliability, security, and performance of cloud environments.

Currently upskilling **Agentic AI**, **AIOps and AI-driven observability** for proactive incident detection, anomaly detection, and predictive analytics in complex cloud ecosystems.

Proven track record in **performance optimization, disaster recovery, and security compliance** across banking, telecom, and e-commerce domains. Adept at driving automation, reducing **MTTR**, and improving operational efficiency through strategic planning and advanced monitoring frameworks.

Work Experience

Team Leader, *SLK Software*
01/2025 – Present
Client: Emerson, Fifth Third Bank, HNB bank | Bengaluru

Emerson

- Built end-to-end **observability** for Azure workloads using **Managed Prometheus, Grafana, Azure Monitor**; **MTTR ↓ 25%**, false alerts **↓ 30%**.
- Designed monitoring for **AKS**, **PostgreSQL**, and HTTP endpoints with **SLO/SLA** dashboards and actionable alerting.
- Delivered infrastructure changes via **Terraform & Ansible** with standardized modules, approvals, and guardrails to improve release safety.
- Collaborated with product owners & platform teams to define **golden signals** and operational readiness checklists for new services.

Fifth Third Bank

- Automated **OS patching & deployments** with **Ansible + Jenkins**; manual effort **↓ 70%**.
- Enabled event correlation and auto-baselining in Dynatrace, cutting P1/P2 incidents by ~20%.
- Introduced **runbooks** and **incident response** playbooks with **PagerDuty/Opsgenie**, improving on-call consistency and time to mitigation.

Skills

• Provisioning infra using Terraform.
• AI observability (OpenAI, Gemini, NVIDIA) and anomaly detection (AIOps).
• Implemented AI-powered automation and self-healing workflows for operational efficiency.
• Predictive analytics for capacity planning.
• Diagnosed Java performance issues (memory leaks, GC pauses, slow endpoints) in production and Monitored JVM health (heap, GC, thread count, response time).
• Performance Tuning and Optimization.
• Disaster Recovery and High Availability.
• Configuration Management and Deployment- Ansible.
• Monitoring, Logging and Observability.
• CI/ CD and Automation.
• Migrating monolithic application to Containerization and Orchestration based model.
• Security and Vulnerability Management.
• Ticketing, Documentation and Collaboration tools.
• On call Production support & IT operations Troubleshooting and Debugging.

Tools

AIOps & Observability AI:
- Dynatrace Davis AI (Anomaly Detection, Root Cause Analysis)
- Splunk ML Toolkit (Log & metric-based anomaly detection)
- Predictive capacity analytics (CPU, memory, pod saturation forecasting)

AI / LLM Skills: Prompt Engineering, Llama / open-source LLMs, Agentic AI workflows, Fast API, LlamaIndex
Operating Systems: Linux, Windows
Servers & Web: NGINX, Apache HTTP, Apache Tomcat, JBoss
Cloud Services: AWS, GCP, Azure
Configuration & Infrastructure Management: Ansible, Ansible Tower, Terraform
CI/CD Tools: Jenkins, Harness CI/CD, Argo CD
Container Technology: Docker, Docker-Compose, Kubernetes, Helm
Database: PostgreSQL, MySQL, RDS

- Acted as a **Build & Release–focused SRE**, owning CI/CD pipelines and production release workflows to ensure releases were **safe, observable, and reversible** across Kubernetes platforms.
- Designed and enforced **release SLOs and post-deployment health checks** using Prometheus, Grafana, Dynatrace, and Splunk to detect bad releases early, reducing rollback frequency and improving MTTR by 25–40%.
- Implemented **blue-green and canary deployment strategies** on EKS/GKE/AKS with capacity-aware rollouts (HPA/VPA), minimizing blast radius and operational risk during high-traffic production releases.

HNB Bank
- Orchestrated event-driven remediation (PowerShell/ Ansible) triggered by anomaly signals, **lowering manual toil by ~30%**.
- Applied OS hardening & patch compliance for cloud and on-prem nodes aligned to CIS baselines; improved audit scores to 95%+.
- Expanded **Dynatrace** & **Splunk** dashboards with threshold tuning and business KPIs; improved signal-to-noise ratio for alerting.
- Managed **GKE** deployments with **HPA/VPA**, resource governance, and secure ingress/egress; improved stability and cost efficiency.

SRE/Devops Engineer, *Impetus Technologies*
06/2021 – 12/2024 | Client: Transunion | Noida
- Migrated legacy monoliths to **Kubernetes microservices** (Docker + GKE, EKS), improved scalability, resilience, and release velocity.
- **Cloud networking & security**: Designed **VPC/VNet** with private subnets, secure ingress (**ALB/App Gateway**), controlled egress (**NAT/Firewall**); removed public exposure for core services.
- Implemented **IAM/RBAC** & **secrets management** (**AWS KMS / GCP Secret Manager**) integrated with CI/CD; enforced least privilege and automated key rotation.
- Implemented production-grade **CI/CD pipelines** using Jenkins, incorporating blue/green and canary deployments, reducing rollback frequency by 30%.
- Developed **Ansible Playbooks** to automate software provisioning, deployment, configuration updates, and system maintenance, reducing manual intervention.
- Tuned **HPA/VPA** and resource requests/limits; lowered compute costs by **~20%** while meeting p95 latency targets.

Monitoring & Logging Tools: Grafana, Prometheus, Cortex, Fluentd, Filebeat, Netdiagnostic, Splunk, ELK Stack, Dynatrace, Google Cloud Monitoring, Amazon CloudWatch, ThousandEyes, AI observability
Security & Vulnerability: SonarQube, Rapid7 Nexpose, CrowdStrike Falcon
Ticketing Tools: JSM, ServiceNow
Version Control: GitHub, GitLab
Incident Management & Automation: PagerDuty, Opsgenie, StackStorm, Shell scripting, AWX
Artifact & Image Management: Docker Trusted Registry (DTR), Harbor, Nexus
Messaging & Streaming: RabbitMQ, ActiveMQ, Kafka
Documentation & Collaboration: Confluence, SharePoint, Google Workspace, Microsoft Teams + OneNote
VPN Solutions: Libreswan, StrongSwan

- Standardized **Terraform modules** for network, compute, and Kubernetes add-ons; cut provisioning time by **~80%** and improved reproducibility.
- Leveraged **Splunk/ELK** for log analytics with custom dashboards; accelerated troubleshooting and reduced mean time to detect.
- Conducted **vulnerability assessments** and applied necessary patches to mitigate security risks and ensure compliance.
- Utilized **Prometheus, Grafana, and Dynatrace** for real-time monitoring and alerting, enabling proactive system management and performance optimization.
- Configured and deployed **VPN solutions** for customers using **Libreswan and StrongSwan**.
- Migrated VMWare to AWS; used EC2, ELB, S3, RDS.
- Managed customer tickets and provided **Oncall supports** for alerts, ensuring timely resolution and customer satisfaction.
- Mitigated **security risks** by conducting regular vulnerability assessments and applying necessary patches.

Software Engineer, *Cavisson Systems*
10/2018 – 05/2021 | Client: Kohl's | Noida

- Implemented robust **monitoring (APM,) and alerting tools** to reduce system downtime for critical applications.
- Performed **performance testing, monitoring, and diagnostics** to optimize enterprise app reliability and throughput.
- Implemented **Jenkins CI/CD** pipelines for build/test/deploy, improved automation and release cadence.
- Provisioned environments using **Terraform**; established logging/monitoring baselines and monthly patch workflows.
- Containerized workloads with **Docker/Docker-Compose**; streamlined packaging and deployment.
- Managed configuration, change, release, and build processes on **Linux**, maintaining system integrity and uptime.
- Worked with software development and testing team members to design and develop robust solutions to meet **client requirements** for functionality, scalability, and performance.