Arun Sanna

arun.sanna@outlook.com
https://www.linkedin.com/in/arunchowdary/

Significant experience:

Served as Architect and Top Contributor largest Platform-as-a-Service (PaaS) platform PartyBus in the U.S. Department of Defense (DoD), operated by the United States Air Force. The **DoD Enterprise DevSecOps platform** supports over **300 defense applications** across multiple classification domains. I designed and implemented a **highly available infrastructure** managing **1,000+ virtual machines**, integrating **Zero Trust security architecture**, **NVIDIA GPU-based workloads on Kubernetes**, and **automated CI/CD pipelines**. This enterprise-scale platform streamlined application deployment while ensuring strict security compliance, enabling the rapid delivery of mission-critical defense systems. Innovations in platform design significantly reduced deployment times and set new standards for **secure, efficient, and scalable software delivery within the DoD**.

Accomplishment: "*Led a pivotal role in Operation Allies Refuge, orchestrating emergency deployment of mission-critical communications platforms within hours. Our platform's rapid scaling and 24/7 support enabled USAF and NATO forces to coordinate the evacuation of 120,000+ souls to Qatar in just 72 hours - marking the largest airlift evacuation in U.S. history. The platform's resilience under extreme pressure and unprecedented user load directly contributed to saving thousands of lives during this historic humanitarian mission.*"

CMS Office of IT Customer Enablement Team Lead: **Led the Customer Enablement Team** within the **CMS Office of IT**, focusing on **migration and modernization initiatives** as part of a **DevSecOps Software Factory** effort. Over the past year, our team developed a **scalable, reusable platform** to streamline **application modernization**, successfully assisting **five applications** in their transition. This initiative resulted in a **40% reduction in costs**, significantly **accelerated release frequency** from **months to days**, and enabled **weekly deployments**, enhancing **time-to-value**. Additionally, I played a **key role in AI integration**, supporting the **CMS AI Team** by enabling the deployment of **Llama models** on an **NVIDIA-based cloud infrastructure**, allowing **data scientists to securely host and utilize large language models (LLMs)**. I implemented the **entire infrastructure using Terraform** and leveraged **EKS with GPU nodes** to enhance **AI and machine learning capabilities**. Furthermore, I built and managed a **JupyterHub environment** to support **fraud detection in Medicare payments**, empowering **data scientists to conduct advanced analytics** and develop **AI-driven chatbots using GenAI** for **end-user support**. In addition, I contributed to **AI-driven security enhancements** by integrating **SBOM-based AI tools**, enabling **automated CVE scoring**, **dependency scanning**, and ensuring that **no vulnerable libraries** were included in packaged software.

Expedited CMS Application Modernization: Led a cross-functional team of 25 engineers, providing mentoring, performance feedback, and hands-on career development for team members. in achieving CMS's fastest-ever application migration and ATO certification - condensing an **18-month process into 90 days** doing it in parallel for **5 Apps with 50+ microservices.** Orchestrated Infrastructure, CI/CD, Security, and Customer Enablement streams to revolutionize the federal compliance process through automated security controls and standardized pipelines. **Maintained 24/7 operational support** while managing complex cross-team dependencies and federal requirements. This achievement set a new benchmark for federal application deployments and established new standards for rapid ATO acquisition without compromising security, becoming a model for future CMS modernization efforts.

Analysis of Alternatives (AoA): As a key member of **Technical Oversight Committees** at both the Department of Defense **United States Air Force and Centers for Medicare and Medicaid Services**, led comprehensive Analysis of Alternatives (AoA) for enterprise application modernization. Evaluated cloud service models (IaaS, PaaS, SaaS) and deployment architectures across AWS and Azure platforms, analyzing performance, security compliance, scalability, and TCO. These strategic assessments drove data-driven recommendations that established the foundation for current cloud infrastructure strategies, optimizing resource utilization while ensuring strict federal compliance standards.

Our team **designed and implemented AI-driven cloud modernization strategies**, successfully transitioning **300+ enterprise applications** to the **cloud with 99.99% uptime**, while embedding **AI and ML capabilities** across **hybrid environments**. We **engineered NVIDIA GPU-powered Kubernetes clusters**, enabling **data scientists to train and deploy large language models (LLMs) like Llama** in a **secure, high-performance cloud environment**. To enhance **fraud detection in Medicare payments**, we built and managed **AI-enabled JupyterHub environments**, allowing real-time **anomaly detection and predictive analytics**. Additionally, our team integrated **AI-powered security automation**, incorporating **Software Bill of Materials (SBOM) tools** to execute **automated CVE scoring, threat detection, and dependency validation**, ensuring **federal-grade security compliance**. By leveraging **serverless AI architectures**, we optimized resource allocation and reduced **infrastructure costs by 35%**, enabling **scalable and cost-efficient AI workloads**. These innovations also included **AI-driven chatbots** for **automated customer support**, improving **user engagement and accessibility** within CMS systems.

In addition to AI advancements, we **led large-scale hybrid cloud and DevSecOps transformations**, achieving a **60% reduction in deployment time** and an **80% improvement in resource utilization** through **containerization (ECS/EKS)**. Our team **automated 100% of infrastructure provisioning** using **Terraform and CloudFormation**, while integrating **AI-driven predictive analytics** into **GitLab CI/CD pipelines** to **identify potential code vulnerabilities and optimize release strategies**. The implementation of **Zero Trust security architectures** leveraged **AI-based anomaly detection** for **automated threat mitigation and real-time compliance enforcement**. We also played a key role in **applying AI models to automate security audits**, reducing **manual compliance efforts by 70%**. Through collaboration and innovation, our team has **set new federal benchmarks** in **AI-driven cloud modernization and security automation**, ensuring **mission-critical defense and healthcare systems operate with unparalleled efficiency, intelligence, and resilience**.

My commitment to innovation and excellence in cloud architecture is evidenced by my hands-on experience and continuous learning. I invite you to review my portfolio at www.github.com/arunsanna, showcasing my journey in leveraging cloud technologies to transform business landscapes.

Education:

- Diploma in Electronics and Communication Engineering (2008-2011), Govt Polytechnic College, Andhra Pradesh.
- Bachelor’s degree in information technology (2011-2014), Jawaharlal Nehru Technological University.
- Master’s in electrical engineering (Computers and Networks) (2014-2015), California State University, Los Angeles.

Certifications:

- Certified Kubernetes Administrator.
- NVIDIA Certified AI Infrastructure and Operations
- AWS Certified Solutions Architect Professional.
- Google Cloud Certified Professional Architect.
- Azure Certified Solutions Architect Expert.
- IBM Certified Associate Developer, WebSphere.
- Microsoft Certified Technology Specialist.

Technical Skills:

Cloud Service Providers	AWS, Azure, and Google Cloud
Kubernetes Distributions	EKS, GKE, AKS, Rancher, Openshift, Konvoy, RKE2, K3s, VMWare TKG.
Infrastructure as Code	Terraform, Open Tofu, Terragrunt, Cloud Formation, Azure Template, and Cloud Deployment Manager
Configuration as code	Chef, Ansible, and Puppet
Infra Testing	Inspec, ServerSpec, Clair and RSpec
Script	Bash & PowerShell
Programming	Python, Ruby, Groovy, Go, AWS CDK and SDK.

Version Control	Gitlab, Github, Bitbucket, SVN, Cloud Source repositories, Code Commit.
Program Management	Jira, Confluence, Trello, Gitlab, Mattermost, Jitsi, and Slack Bots.
CI/CD	CodeBuild (GCP), Jenkins CI, Gitlab CI, Travis CI, FluxCD, Jenkins, ArgoCD
AI Enablement	AWS Bedrock, Sagemaker, Azure OpenAI,Azure Machine Learning, Jupyterhub, Terraform for AI, EKS/GKE/AKS with GPU, RAG Local and Cloud, Tensorflow, Pytorch, CUDA, Langchain, Kubeflow, NVIDIA A100 & H100 GPU's, RAPIDS, Triton and Clara
K8s Administration & Management	Helm, Kyverno, OPA, Kustomize, Grafana, Jaeger, Istio, Nginx, GateKeeper, Velero, Vault, Sops, NVIDIA GPU Operator and Kiali
Container Runtimes	Docker, CRI, Rocket, Podman, Buildah.
Security & Audit Tools	Anchore, OPA GateKeeper, Twistlock, Nessus Manager, and OpenSCAP.
Databases	MySQL, Oracle, Elastic Search, MSSQL, Mango DB, Cosmos DB, Dynamo DB, Redis, RedShift, and PostgreSQL.
Operating Systems	RHEL7, RHEL8, Centos, Ubuntu, and Windows.
Amazon Web Services	**Computing Services** (EC2, ECS, EKS, Lambda, Elastic Beanstalk, Auto Scaling, EC2 Image Builder). **Storage Services** (S3, EBS, EFS, FSx, Storage Gateway, Snow Family, S3 Glacier). **Database Services** (RDS, DynamoDB, ElastiCache, Neptune, Redshift, DocumentDB, Timestream). **Networking Services** (VPC, Route 53, CloudFront, API Gateway, Direct Connect, Global Accelerator, Transit Gateway). **Security Services** (IAM, WAF, Shield, KMS, Secrets Manager, Certificate Manager, GuardDuty, Security Hub, Inspector). **DevOps Services** (CodePipeline, CodeBuild, CodeDeploy, CodeCommit, CodeArtifact, Cloud9, CloudFormation, Systems Manager). **Monitoring Services** (CloudWatch, CloudTrail, Config, X-Ray, Managed Grafana, Managed Service for Prometheus). **Analytics Services** (EMR, Kinesis, Athena, QuickSight, OpenSearch Service, Lake Formation, Glue). **AI/ML Services** (SageMaker, Comprehend, Rekognition, Polly, Textract, Lex, Forecast, Personalize, Kendra, CodeGuru, SageMaker Ground Truth).
Google Cloud Services	**Computing Services** (Compute Engine, GKE, Cloud Run, App Engine, Cloud Functions, VMware Engine, Batch). **Storage Services** (Cloud Storage, Persistent Disk, Filestore, Transfer Service, Storage Transfer, Cloud Backup & DR). **Database Services** (Cloud SQL, Cloud Spanner, Cloud Bigtable, Firestore, Memorystore, AlloyDB, Cloud Datastore). **Networking Services** (VPC, Cloud Load Balancing, Cloud CDN, Cloud DNS, Cloud Interconnect, Cloud VPN, Network Service Tiers). **Security Services** (Cloud IAM, Cloud KMS, Secret Manager, Security Command Center, Cloud Armor, Identity Platform, Binary Authorization). **DevOps Services** (Cloud Build, Cloud Deploy, Artifact Registry, Cloud Source Repositories, Container Analysis). **Monitoring Services** (Cloud Monitoring, Cloud Logging, Cloud Trace, Cloud Profiler, Cloud Debugger, Error Reporting). **Analytics Services** (BigQuery, Dataflow, Pub/Sub, Dataproc, Data Fusion, Looker, Data Catalog). **AI/ML Services** (Vertex AI, Vision AI, Speech-to-Text, Natural Language AI, Translation AI, AutoML, Document AI, Contact Center AI)
Azure	**Computing Services** (Azure VMs, AKS, Container Instances, App Service, Functions, Batch, Service Fabric). **Storage Services** (Blob Storage, Disk Storage, Files, Archive Storage, Data Box, StorSimple). **Database Services** (SQL Database, Cosmos DB, Database for MySQL/PostgreSQL, Cache for Redis, Time Series Insights). **Networking Services** (Virtual Network, Load Balancer, Application Gateway, CDN, ExpressRoute, DNS, Traffic Manager). **Security Services** (Active Directory, Key Vault, DDoS Protection, Security Center, Sentinel, Defender, Information Protection). **DevOps Services** (DevOps, Pipelines, Repos, Artifacts, Boards, Test Plans, Azure DevTest Labs). **Monitoring Services** (Monitor, Log Analytics, Application Insights, Network Watcher, Service Health). **Analytics Services** (Synapse Analytics, Data Factory, HDInsight, Databricks, Stream Analytics, Power BI). **AI/ML Services** (Machine Learning, Cognitive Services, Bot Service, OpenAI Service, Computer Vision, Language Understanding). **Integration Services** (Logic Apps, Service Bus, API Management, Event Grid, Event Hubs).

Experience

VivSoft Technologies LLC (Chief Architect)
06/2019 – Current

Strategic Business Development & AI Innovation
Spearheaded the integration of AI-driven automation across enterprise workflows, reducing operational turnaround times by **60%** through the design and deployment of custom OpenAI-powered applications built on **LangChain, LangFlow, and Flowise frameworks**. Developed intelligent systems automating proposal generation, compliance analysis, and market trend evaluation, enhancing response quality while eliminating 25+ hours of manual work weekly. Championed organization-wide AI adoption through hands-on training programs and cross-functional collaboration, directly contributing to the expansion of our technical portfolio into **generative AI, machine learning pipelines, and intelligent process automation**. Concurrently supported business development initiatives by leveraging AI-analyzed market data to optimize client engagement strategies, resulting in a **30% increase** in qualified opportunity pipeline growth and strengthened competitive positioning.

Principal Cloud DevOps Architect – Centers for Medicare and Medicaid (CMS)
Led and mentored a diverse team of engineers, focusing on skill development, performance feedback, and career growth, resulting in a 30% improvement in team efficiency and a 25% reduction in project delivery times.
Engineered and automated cloud-native solutions on AWS, Azure, and Google Cloud, integrating AI and ML capabilities to enhance operational capabilities and ensure highly reliable, scalable deployments.
Spearheaded the development of intelligent automation tools that cut manual work by over 25 hours per week, using frameworks like LangChain, LangFlow, and Flowise for AI-powered proposal generation and market trend evaluation.
Designed and delivered **highly reliable automated pipelines** for infrastructure deployment, testing, and image publication, ensuring smooth cloud service operations with a focus on performance and security.
Fostered a collaborative agile engineering culture, using **Scrum and Kanban** methodologies to improve team output and align development efforts with business objectives.

My responsibilities include:

- Building reusable platforms, such as a production-ready EKS platform that integrates with the CMS network and meets SecOps compliance standards.
- Developing Terraform Infrastructure as Code (IaC) modules for provisioning components like MySQL, MSSQL, PostgreSQL, EFS, Redis, and S3, streamlining infrastructure setup and reducing redundancy.
- Creating comprehensive training materials for customers and teams to ensure effective platform and service utilization.
- Automating monthly node rotations with new compliance VM images to maintain security and efficiency.

Played key role and constructed a DevSecOps software factory to provide DevSecOps services, enabling continuous application authorization. Leading the customer enablement team, lead modernization of applications running in data centers or monolithic architectures by embedding team members into the application teams using the Sherpa model. We implement automation with Terraform and Terragrunt and develop CI pipelines that guide application changes through quality and security checks, deploying them using the GitOps model.

Key achievements include:

- Subject Matter Expert (SME) CMS OIT IUSG Modernization Initiative.
- Modernization of 5 Apps with 50+ Jenkins Pipelines, 50 containers combined in 90 days, Record time in CMS.
- Integrated open-source tools to streamline application builds.
- Constructed highly available Kubernetes clusters on EKS with enterprise DoD Enterprise Software factory reference design. Designed and deployed high-availability Kubernetes clusters (EKS, GKE, AKS, RKE2) integrated with service mesh and zero trust security models, enabling real-time mission-critical operations.
- Authored over 50+ reusable IaC modules to enhance operational efficiency. Developed Infrastructure as Code (IaC) solutions using Terraform and CloudFormation, and recently expanded expertise into AWS CDK and OpenTofu for cloud-native provisioning and automation.

- Pioneered rapid application modernization, reducing ATO timelines from 18 months to 90 days while ensuring compliance with both federal (FedRAMP) and financial regulatory standards (SOC2, ISO 27001).
- Expanded IaC capabilities by incorporating AWS CDK and OpenTofu alongside Terraform and Ansible to streamline infrastructure provisioning and compliance enforcement.
- Developed reusable automated pipelines for 100% seamless infrastructure deployment.
- Architecting and managing diverse environments (Dev/Staging/Prod) using parameterized, reusable templates.
- Migrated and containerizing applications into Helm charts for Kubernetes.
- Deployed a highly available, self-hosted GitLab and GitLab CI for centralized development and build pipelines.
- Created project templates to expedite migration and modernization processes.
- Leading customer enablement to assess and modernize 10 applications, transitioning them to containerized environments and evolving into microservice architectures.
- Integrating applications with CMS Okta SSO for streamlined with existing identity management.
- Utilizing AWS services for efficient data transfer from on-premises to the cloud.
- Implementing comprehensive testing and analysis practices, including secrets scanning, static and dynamic code analysis, unit testing, code coverage, user acceptance, and performance testing.
- Developing an A/B release strategy for seamless production changes, minimizing downtime.
- Crafting Security Groups (NSGs) to regulate traffic for network interfaces, VMs, and subnets.
- Fostering infrastructure that supports microservices with Istio service mesh to implement mTLS.
- Integrating security tools for automated SAST, DAST, vulnerability scanning, build automation, secrets scanning and SBOM.
- Bridged security compliance frameworks between DoD (FedRAMP, RMF) and enterprise financial standards (SOC2, PCI DSS), ensuring seamless security automation across multi-cloud environments.
- Implementing robust encryption and Zero Trust architectures to safeguard against unauthorized access.

Principal Cloud DevOps Architect – DoD USAF (United States Air Force) PlatformOne

- Principal anchor, Lead and subject matter expert for the DoD Enterprise DevSecOps Initiative. Able to build Largest DoD Platform that host mission critical applications and weapon systems combined 300+ Applications.
- SRE for multiple Kubernetes clusters hosting major DoD weapon systems at Platform One at multiple classification levels.
- Created the first DoD Enterprise DevSecOps managed service platform with Kubernetes that can run on any cloud platform AWS, Azure, GCP, and On-Prem.
- Contributed and Largest contributor till date(2/1/2025) to PlatformOne PartyBus (production-ready managed secured K8s platform), BigBang (application stack monitoring, logging, and security), and IronBank (3000+ hardened containers).
- Bridged security compliance frameworks between DoD (FedRAMP, RMF) and enterprise financial standards (SOC2, PCI DSS), ensuring seamless security automation across multi-cloud environments.
- Implemented an advanced cybersecurity stack with a sidecar container security stack, leveraging a Service Mesh and enforcing Zero Trust security down to the container level.
- Demonstrated containerization of weapon systems, including jets and space systems, transforming real-time OS and legacy hardware.
- Developed automated security governance pipelines aligning DoD STIG hardening standards with financial security compliance frameworks, facilitating secure DevSecOps adoption in highly regulated environments.
- Integrated AI/ML capabilities to enhance Air Force jets, providing co-pilot functions.
- Achieved high-quality, secure software delivery with exceptional DORA metrics.
- Containerized legacy applications and built Helm Charts for automated scaling.
- Developed robust storage solutions for multiple applications on Kubernetes.
- Utilized Terraform and Terragrunt for IaC deployments, enabling Kubernetes on RKE2 within AWS environments.
- Transitioned multiple applications into Helm charts for streamlined deployments.
- Served as SRE for over 20 VM-based Kubernetes clusters, managing 300+ applications with 1000+ VM's.
- Automated the deployment of HA RKE2 Kubernetes clusters using Terraform and Terragrunt.
- Empowered engineers to rapidly develop, build, and certify applications.
- Managed critical applications and tools, ensuring optimal performance and security.
- Deployed secure Kubernetes clusters in AWS and Azure, leveraging IaC for consistency and compliance.
- Executed Kubernetes deployments using EKS, AKS, and GKE.
- Integrated Kubernetes deployments with identity management and storage solutions.
- Scripted Kubernetes deployment using Rancher for Government (RKE2), establishing a continuous Authority to Operate (CATO) compliant infrastructure.

- Configured Keycloak for SSO, SAML, and OIDC for applications.
- Architected comprehensive monitoring infrastructure using open-source stack (Grafana, Prometheus, Loki) achieving 99.9% system visibility. Implemented intelligent alerting through integration with communication platforms, enabling proactive incident response with 15-minute Mean Time to Detection (MTTD). Established automated remediation workflows reducing Mean Time to Resolution (MTTR) from hours to minutes while saving $2M annually in proprietary monitoring costs.
- Implemented Kubernetes-based mission-critical applications on Azure, GCP, and AWS, using Terraform.
- Deployed managed GKE clusters using Terraform, integrating core functionalities like monitoring, logging, security, and CI/CD.
- Bridged On-Prem and Cloud Kubernetes clusters using Anthos, configured Istio with multiple gateways, and enforced zero trust security with envoy proxy.
- Established comprehensive permissions structures and configured SAML and OIDC clients for SSO integration.
- Implemented Prometheus for monitoring and alerts.
- Authored custom Helm charts for Istio, enabling a secure network mesh with zero trust architecture.
- Configured logging using Fluentbit, Elasticsearch, and Kibana for centralized log management.
- Maintained a Kubernetes-based GitLab repository and registry.
- Developed CI/CD pipelines within Git and automated deployments using GitLab runners.
- Crafted hardened container images for applications like GitLab, Fortify, SDElements, Jira, and Confluence.
- Engineered solutions for deploying Kubernetes in air-gapped systems.
- Designed logging solutions with Elasticsearch, Fluentbit, and Kibana.
- Developed Helm charts for Jira and Confluence tailored for DoD Kubernetes clusters.
- Facilitated the migration of workloads from VMs to Kubernetes clusters.
- Engineered highly available, scalable, and fault-tolerant applications.
- Applied chaos engineering principles to test application resilience.
- Guided clients through the cATO process within DevSecOps frameworks.
- Implemented zero trust security using Istio mTLS, SPIFFE, and SPIRE and Managed secrets using Vault and SOPS.
- Deployed cluster autoscaler for dynamic resource adjustment and Integrated shared storage solutions, including Rook/Ceph and EFS, into Kubernetes clusters.

Hitachi Vantara
10/2018 – 06/2019

Sr. DevSecOps and Data Science Engineer

- **Implemented Department of Defense Security for the USTRANSCOM project**. Part of the core team that implemented the DISA Secure Cloud Computing Architecture (SCCA) framework from scratch on AWS GovCloud for the first time. That work involved integrating security tools to automate application scanning for vulnerabilities. Built encryption capabilities and Zero Trust to prevent malicious access
- Converted and created many GCP environments in IAC using terraform and built several reusable modules that can be shared between projects and completed eliminated duplication of work.
- Led migration of Virtual Machines to Azure Virtual Machines for multiple global business units.
- **Prepared capacity and architecture plan** to create the Azure Cloud environment to host migrated IaaS VMs and PaaS role instances for refactored applications and databases.
- Configured VMs in availability sets using Azure portal to provide resiliency for IaaS based solution and scale sets using Azure Resource Manager to manage network traffic.
- Deployed and managed MySQL, PostGres, SQL Server using Cloud SQL and Spanner in GCP.
- Created shared VPC's and Automated Peering process using terraform in AWS and GCP.
- Configured and managed VPN's, Dedicated Interconnect, Partner Interconnect in GCP.
- Created Autoscaling based on CPU metrics, Configured Load balancing with SSL termination and configured CDN's in GCP and AWS
- Developed a product that can read all Jira and tempo data, which will give visibility for the project managers about employee work allocations in each project and bench pool candidates with skillset can be allocated to new

projects, which changed the company's internal project assignments. The best part is its prediction of teams with employees facing hardship with employees who can help them.

- Provisioned Machine Learning and Artificial intelligence Infrastructure using Kubeflow on Kubernetes for a data scientist to create prediction models using jupyter notebooks
- Experienced with KIAM, AAD Pod Identity management, Azure Identity Services, and AWS Identity access management.
- Experienced with Ingress controllers in Kubernetes like Nginx, istio, and traefik.
- Familiar with Jira and Confluence project management and tracking tools.
- Provisioned highly available Splunk and sensu Monitoring and Logging Servers using chef servers.
- Experienced with **version control tools like git, GitLab, and code commit.**
- Built STIG'ed (Hardened Images) using DISA Guidelines.
- Wrote several Inspec Profiles to run validation tests against instances to verify and validate for compliance.
- **Helped team to embed security and hardening** while designing and developing pieces of infrastructure. Wrote Packer templates to build base golden images which are created with all necessary tools and security patches done before the team used them for any development or deployment.
- Designed and configured Azure Virtual Networks (VNets), subnets, Azure network settings, DHCP address blocks, DNS settings, security policies and routing.
- Deployed Azure IaaS virtual machines (VMs) and Cloud services (PaaS role instances) into secure VNets and subnets.
- Exposed Virtual machines and cloud services in the VNets to the Internet using Azure External Load Balancer.
- Associated routes with VNets via the route table per relationship constraints.
- Managed IP Forwarding for VMs and role instances acting as virtual appliances.
- Created ARM Templates to deploy workloads in Azure.

REAN **Cloud**
03/2015 – 10/2018

DevSecOps and Data Science Engineer

Responsible for working closely with the Product Development, DevOps, Data Science, and Delivery teams to automate the infrastructure provisioning using terraform, python, and ruby. Developing CHEF cookbooks and Inspec/ServerSpec and AWS profiles to validate infrastructure. Create automation for deployments, which will enable push-button deployments, which will reduce deployment time. Participating in Design discussions to review architectures to reduce complexity in applications and make them more efficient.

- Built Cloud formation templates for Amazon, to support customers to get the taste of cloud services. Multiple templates that will deploy stacks with webservers and databases in a fully automated way.
- Wrote several chef cookbooks, to automate the installation of Web Servers, Application Servers, and databases. Personally, converted several admin manuals into chef cookbook so you don't need to read pdf documents again.
- Built Infrastructure as code using Terraform. Helped Client Ellucian with more than 100 products.
- Helped them to design cloud application architecture. Helped team to build IAC using terraform ground up.
- Designed Highly Available and fault-tolerant applications. Helped Ellucian to build tools to reduce infrastructure expenses.
- Automated end-to-end solution for developers and operations along with security requirements by **creating pipelines for build**, commission, deploy, secure, test, validate and log phases of the sprint using **Ansible**, PowerShell, Jenkins, **Gitlab-CI, Docker, Kubernetes, and Docker swarm tools.**
- Troubleshot network related issues, errors, security ports related issues and automated resolution fixes.
- Planned, identified security ports, protocols, and services, and automated the systems for SecOps based on the requirements.

- **Wrote Ansible Playbooks** for many products at client Ellucian. Helped the engineering team to understand how to decompose configuration as code as building blocks and reusing code across the company. Which reduced engineering time.
- Wrote several packer projects integrated with **Ansible and AWS** to build AMI's in Amazon.
- Imported several data center virtual boxes into AWS.
- Deployed and helped the team to understand the importance, limitations, and workaround for AWS RDS and helped the team to migrate databases.
- Designed Virtual Private networks and designed integrations with other virtual private clouds via gateways and peering's etc.
- Built products around learnt solutions over time.
- Built log aggregation and management using AWS internal services and saved a ton on money paid in licenses to Splunk.
- Utilized Amazon Glacier for archiving data.
- Utilized CloudWatch to monitor resources such as **EC2**, CPU memory, Amazon RDS DB services, DynamoDB tables, EBS volumes; to set alarms for notification or automated actions; and to monitor logs
- Designed roles and groups for users and resources using AWS Identity Access Management (IAM) and managed network security using Security Groups, and IAM.
- Strong advocate of opensource first, unless if there is something that compromises the reliability of the application.
- Wrote many lambda scripts that will automate most of the op's work. Configures SES and SNS with alerting So the Engineering team will get notified.
- **Built a tool with Elastic, Logstash, and Kibana** to analyze the cost patterns and take necessary actions.
- Created terraform modules that will deploy IAC in multi-cloud environments like GCP and Azure to avoid vendor lock-in.
- Converted applications into containers to run them in ECS.
- Helped Engineering teams to understand cloud offerings like **Elastic Container Registry**, Code Commit, Code Pipelines, SQS, and EMR.
- Migration of Peta Bytes of data from on-prem to cloud and wrote programs to validate migration.
- Developed and customized the cookbooks using berks, kitchen, chef-solo, and chef-server
- Performed validation and testing the cookbooks using the kitchen, Inspec, and food critic.
- Wrote power-shell scripts to target the windows AMIs in the AWS and install the windows packages headless and testing them.
- Created and deployed applications in AWS Kubernetes, Azure Kubernetes, and Google Kubernetes Engine.