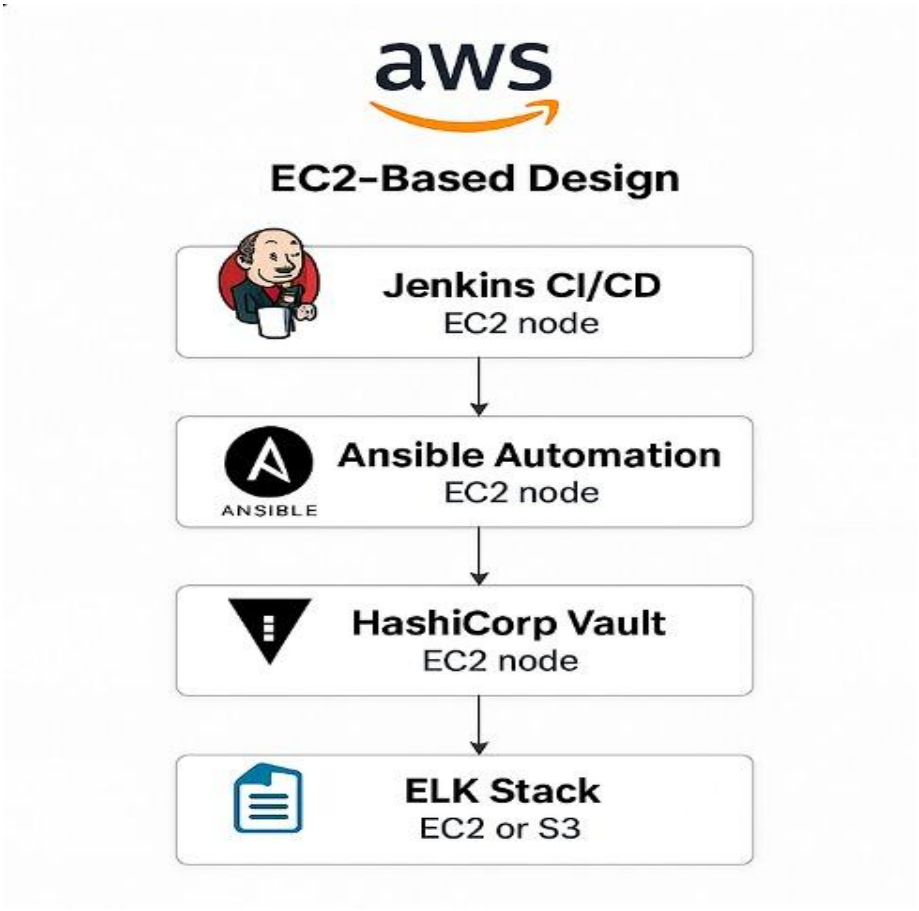

1. **AWS EC2-Based Secure CI/CD Pipeline**: This project deploys a secure document access system using Jenkins for CI/CD automation, Ansible for configuration management, and HashiCorp Vault for secrets management—all hosted on AWS EC2 instances.
2. **End-to-End Automation**: Jenkins triggers Ansible playbooks to enforce access policies, while Vault centrally manages credentials, ensuring least-privilege access to sensitive documents.
3. **Audit & Compliance**: The ELK Stack (Elasticsearch, Logstash, Kibana) aggregates and visualizes Vault audit logs, enabling real-time monitoring and compliance reporting.
4. **Infrastructure-as-Code (IaC)**: All components (Vault policies, Jenkins pipelines, Ansible roles) are defined as code for reproducibility and scalability.
5. **Scalable & Secure**: Designed for cloud-native environments, the system supports dynamic scaling (EC2/S3) while maintaining zero-trust security principles.

Key Tech: AWS EC2, Jenkins, Ansible, HashiCorp Vault, ELK Stack.