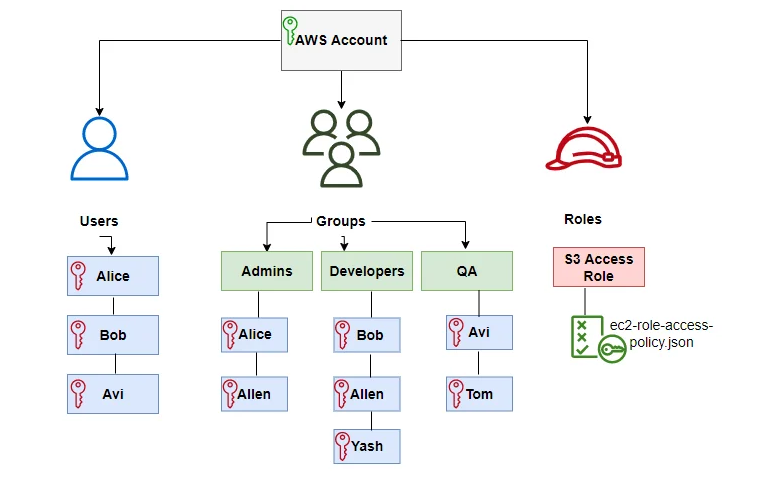
Prepared By – Anmol Singh

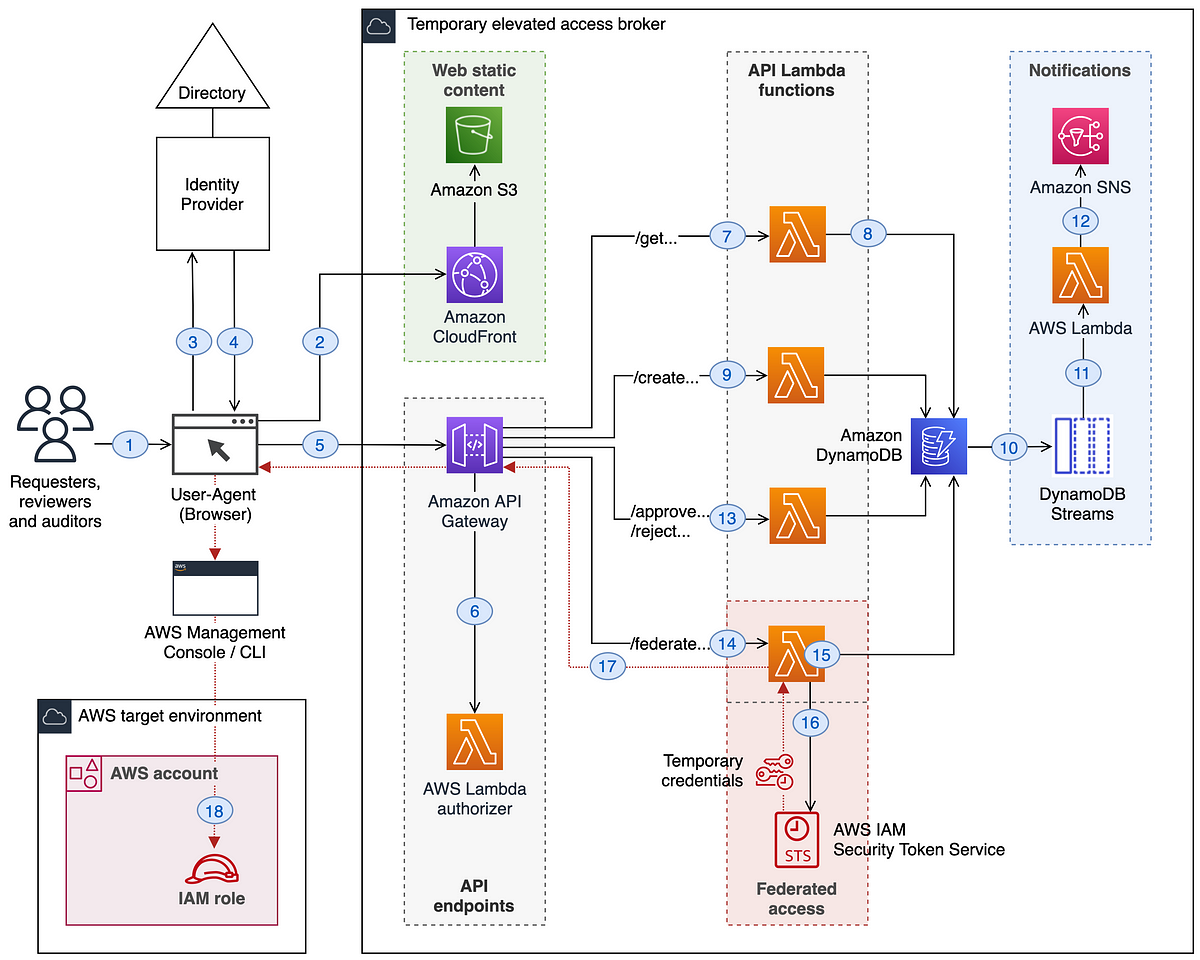
Student Id – 989468785

**AWS Migration Security Architecture**

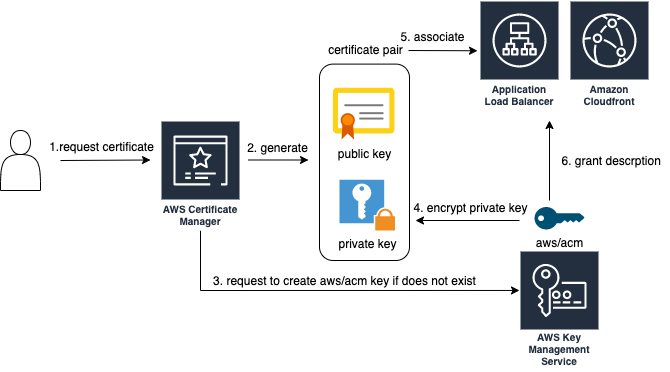
In the migration of eCommerce (Web Application) Product to AWS there are security principles like CIA which is Confidentiality, Integrity and availability which are to be considered and AWS addresses these principles by offering controllability, auditability, visibility, agility, and automation through its tools. The AWS shared responsibility model will help this organisation to adopt the cloud and achieve their security and compliance requirements.

1. **Principle of Least Privilege**: The AWS Identity and Access Management (IAM) will securely control and shares the policies required for individual or group access to the provided AWS resources with least privilege access like authentication and authorization to sensitive data in eCommerce (Web Application). The AWS Identity and Access Management(IAM) has the ability to integrate with other AWS services and also supports multi-factor authentication (MFA), identity management and granular permissions which is a extra layer of protection for eCommerce (Web Application). For eCommerce mobile application AWS Identity and Access Management(IAM) provides AWS Security Token Service (AWS STS) which issues temporary security credentials for job roles.

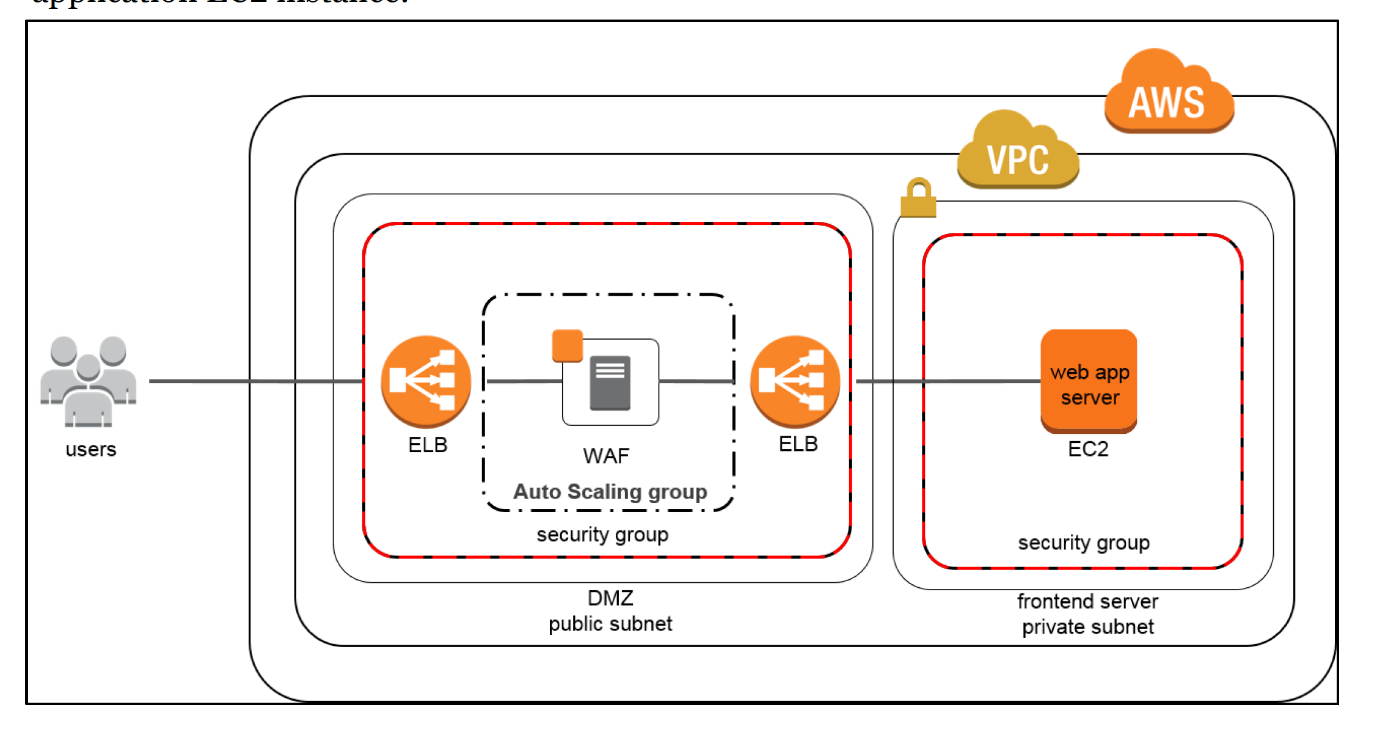
****

****

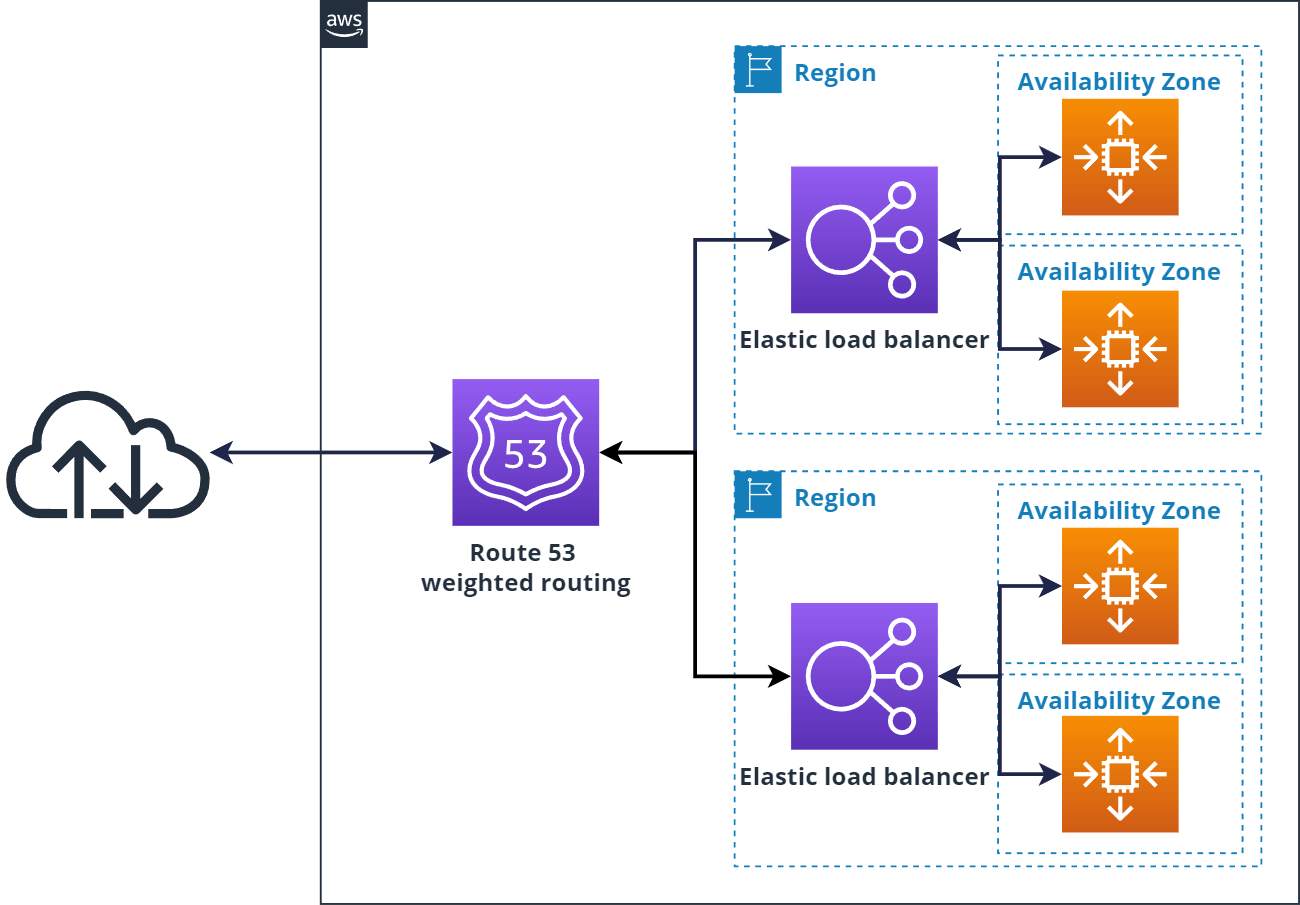
1. **Data Protection**: AWS Key Management Service (AWS KMS) will create and control the cryptographic keys used to encrypt the data in eCommerce (Web Application). AWS will support both client-side and server-side encryption for eCommerce (Web Application). The AWS Certificate Manager (ACM) will provide single interface to deploy and manage both public and private SSL/TLS certificates for data protection in transit for eCommerce (Web Application).



1. **Network Security**: For the secure network of eCommerce (Web Application) there will be implementation of firewalls and segment the network with Virtual Local Area Network (VLAN) or Virtual Private Cloud (VPC) to restrict the access and filter the inbound/outbound traffic which can be done by Amazon Virtual Private Cloud (Amazon VPC) which isolates the network endpoints and configurations to limit the access. Also, AWS Network ACLs will act as a firewall to control and filter inbound/outbound traffic whereas AWS Web Application Firewall (AWS WAF) will provide protection for the eCommerce website from attacks like brute force attacks, Cross Site Scripting (XSS) and SQL Injection.

****

1. **Availability and Scalability**: The Elastic Load Balancer (ELB) will provide the distribution of incoming traffic across multiple targets which includes access from different IP addresses in one or more availability zone and Amazon Cloud Front will provide consumers improved access speed for downloading eCommerce (Web Application).

****

1. **Monitoring and Logging**: The use of Amazon Virtual Private Cloud (Amazon VPC) in eCommerce (Web Application) will provide endpoints of the network to limit access to Amazon S3 buckets and also by AWS Cloud Trail continuous monitoring and logging account activity in eCommerce (Web Application) can be done. Also, the Amazon GuardDuty will help in analysing the entire AWS environment on which the eCommerce (Web Application) is running while Amazon Inspector will provide security assessments for eCommerce (Web Application) settings and configurations.

**The Final eCommerce (Web Application) architecture diagram will be**:

This below diagram describes the final eCommerce (Web Application) architecture by showing the AWS CloudFront for content delivery, Elastic Load Balancing (ELB) and Web Application Firewall (WAF) for load balancing and security, Elastic Compute Cloud (EC2) for hosting the web application, Relational Database Service (RDS) for the database, AWS CloudWatch and AWS CloudTrail for monitoring and logging activity.

