# AWS Architecture Detailed Explanation

## Introduction

This document provides a comprehensive explanation of the AWS architecture designed for hosting a highly available and secure application. The architecture consists of multiple AWS services integrated to ensure performance, security, scalability, and monitoring.

## Architecture Overview

The architecture is designed with high availability, fault tolerance, and security in mind. The system spans across two Availability Zones (AZs) and is divided into three tiers:  
1. \*\*Web Tier\*\*  
2. \*\*Application Tier\*\*  
3. \*\*Database Tier\*\*

## Network Layer

- \*\*VPC (Virtual Private Cloud):\*\* The entire architecture is hosted within a VPC, which logically isolates the network from other AWS customers.  
- \*\*Internet Gateway:\*\* Allows communication between the VPC and the internet.  
- \*\*Route 53:\*\* Manages domain name resolution and routes traffic to the appropriate resources.  
- \*\*CloudFront:\*\* Content Delivery Network (CDN) to serve content globally with low latency.  
- \*\*WAF (Web Application Firewall):\*\* Protects the application from common web exploits like SQL injection and cross-site scripting.

## Web Tier

- \*\*ALB (Application Load Balancer):\*\* Distributes incoming traffic across EC2 instances in two public subnets.  
- \*\*Public Subnets:\*\* Host the EC2 instances that serve the frontend of the application.  
- \*\*Security Groups:\*\* Control inbound and outbound traffic to the instances.

## Application Tier

- \*\*Private Subnets:\*\* Host the backend application instances.  
- \*\*Auto Scaling Group (ASG):\*\* Automatically scales the number of EC2 instances based on demand.  
- \*\*Security Groups:\*\* Ensure only necessary traffic is allowed between the web tier and application tier.

## Database Tier

- \*\*Primary DB (Amazon RDS):\*\* Stores application data with automatic failover to a standby instance.  
- \*\*Standby DB:\*\* Synchronous replication ensures high availability.  
- \*\*Private Subnets:\*\* Secure the database instances from direct internet access.  
- \*\*Security Groups:\*\* Allow traffic only from the application tier.

## Monitoring and Security

- \*\*CloudWatch:\*\* Monitors system performance and logs.  
- \*\*WAF:\*\* Protects the application from attacks.  
- \*\*IAM Roles:\*\* Grant permissions to various AWS services.  
- \*\*Encryption:\*\* Data is encrypted at rest and in transit.

## Conclusion

This architecture ensures a highly available, secure, and scalable environment for the application. It leverages AWS best practices and services to meet the business requirements efficiently.