Project 1: Scalable Web Application with ALB and Auto Scaling

By: Dina Abdelgalil Mohamed
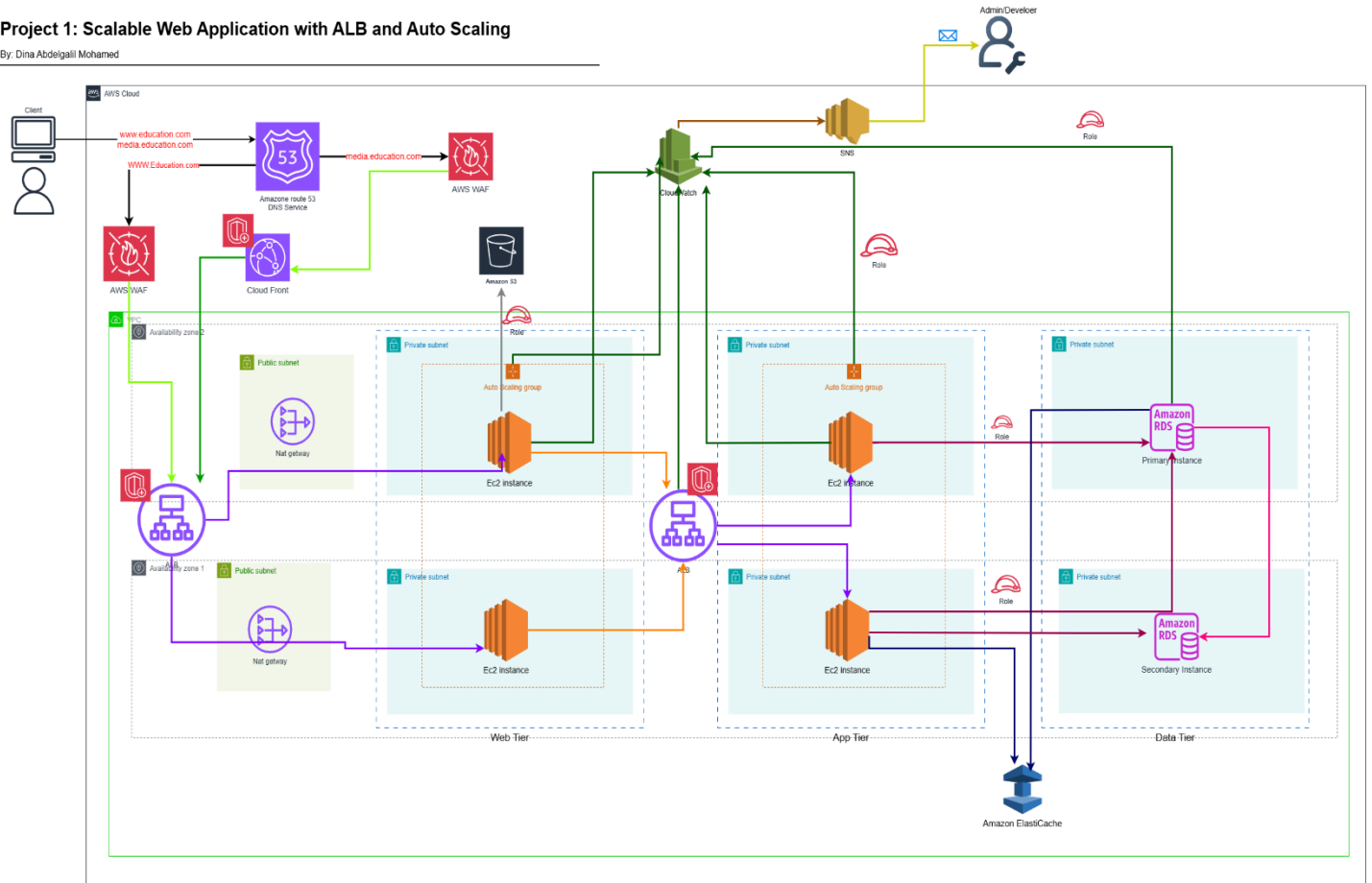
eLearning Platform - AWS Architecture Overview

The **eLearning platform** is designed using a **highly available and scalable three-tier architecture** deployed across **two Availability Zones (AZs)** to ensure fault tolerance and reliability.

Infrastructure Design

1- Networking & Subnets

- The architecture is deployed within a **VPC** containing:
    - **1 Public Subnet**: Contains the **NAT Gateway** allow private instances to access the internet.
    - **3 Private Subnets**:
        - **Web Tier**: Hosts **EC2 instances** serving as web servers.
        - **App Tier**: Hosts **EC2 instances** for business logic processing.

- **Data Tier**: Hosts **Amazon RDS** with Multi-AZ replication. A **Primary instance in AZ1** and a **Secondary instance in AZ2** for failover support.

2- Traffic Routing & Load Balancing

- **Amazon Route 53** directs incoming requests to AWS WAF for security.
- Requests are then routed either to **CloudFront** (for static/media content) or to the **ALB** (for dynamic requests).
- **Application Load Balancer (ALB)** distributes web traffic among **EC2 instances in the Web Tier**, ensuring high availability.

3- Compute & Database Layer

- **Web Tier**: Each AZ contains **one EC2 instance** to handle frontend requests.
- **App Tier**: Each AZ contains **two EC2 instances** to process business logic.
- **Data Tier**:
    - **Amazon RDS (Multi-AZ Deployment)**
    - **Primary instance in AZ1, standby instance in AZ2 for failover support**.
- **Amazon ElastiCache** is integrated to enhance performance by caching frequently accessed data.

4- Security

- **AWS Shield** protects against DDoS attacks on **CloudFront** & **ALB**.
- **AWS WAF** secures **ALB** by filtering malicious requests.
- **IAM Roles & Policies** enforce least-privilege access across services.
- **Amazon S3** is used for file storage, accessed securely by EC2 instances.

5- Security Groups & Network Access Control

Security Groups (SGs) act as **virtual firewalls** to control inbound and outbound traffic for:

- **ALB SG**: Allows HTTP/HTTPS traffic from the internet.
- **Web Tier SG**: Accepts traffic only from ALB SG.
- **App Tier SG**: Accepts traffic only from Web Tier SG.
- **Database SG**: Accepts traffic only from App Tier SG.
- **NAT Gateway SG**: Allows outbound traffic for private instances.

6- Monitoring & Notifications

- **Amazon CloudWatch** collects logs and performance metrics from all services.
- **Amazon SNS** sends real-time notifications to **admins and developers** about system health, security alerts, and performance issues.