Project Proposal: Secure Cloud Network Architecture for Multi-Tier Application

Course Code : CSC472/CSE472

Semester : Summer 2023

Group No : A3

Instructor's Name: Dr. Rubaiyat Islam

Prepared by:

Kazi Mahbub Morshed Limon (2231316)

Rudrita Rahman (2021059)

MD Abu Sauri Sufian (1930839)

MD. Protik Hasan (2022133)

Shatabde Debnath (2020552)

Date : 14th August 2023

Contents

Proposed Project 1
Problem Identification 1
Proposed Solutions and Opportunities 1
Project Goal and Objectives 1
Goal 1
Objectives 1
Project Summary 2
Future Scope: Marketing and Launch 3
System Stakeholders 4
Diagrams 4
Cloud Documentations 6
Security Features 6

Proposed Project

In today's digital era, businesses are increasingly relying on cloud-based solutions to host their applications and services. However, maintaining a robust network architecture and ensuring data security of these cloud-based multi-tier applications remains a significant challenge.

This project proposes to provide services as a cloud service provider of Bangladesh. In this project, we will focus on developing a network with AWS services for an organization (as per their requirements manually). Other than that, for future work we plan on an automatic service so the organizations and business owners can easily deploy their web server, streaming server etc. with proper data security and network segmentation.

Problem Identification

- **Data Security:** Cloud environments are susceptible to security breaches, data leaks, and unauthorized access due to the inherent nature of remote storage and processing.
- **Network Vulnerabilities:** Multi-tier applications require intricate network configurations, which can lead to potential vulnerabilities and inefficiencies.
- **Lack of Standardization:** Many organizations struggle with inconsistent security practices and a lack of standardized approaches to cloud security.
- **Data Loss:** Inadequate data backup and recovery strategies leading to potential data loss.
- **Scalability Challenges:** Scaling applications in the cloud while maintaining security and performance is a complex task.

Proposed Solutions and Opportunities

- **Advanced Encryption:** Implement end-to-end encryption for data in transit and at rest, using industry-standard encryption algorithms.
- **Identity and Access Management (IAM):** Implement robust IAM solutions to manage user roles, permissions, and authentication.
- **Network Segmentation:** Utilize network segmentation to isolate application tiers, limiting the potential impact of security breaches.
- **Intrusion Detection and Prevention Systems (IDPS):** Deploy IDPS to monitor and mitigate threats in real-time.
- **Automation:** Implement automated security protocols for rapid response to potential security breaches or vulnerabilities.
- **Scalability Architecture:** Design an architecture that allows for seamless scalability while maintaining security standards.

Project Goal and Objectives

Goal

To create a secure cloud network architecture that safeguards multi-tier applications against potential threats and vulnerabilities.

Objectives

By implementing a Secure Cloud Network Architecture for Multi-Tier Applications, we aim to provide a robust and scalable solution that ensures the security of data and the reliability of applications in the cloud environment. This project addresses critical security challenges while providing opportunities for enhanced scalability and efficiency.

1. Develop a multi-tier application architecture compatible with major cloud service providers (e.g., AWS, Azure, GCP).

2. Implement robust security measures (e.g., multi-factor authentication, encryption, and micro-segmentation) at each application tier.
3. Design and implement IAM strategies to manage user access effectively.
4. Develop automated security protocols for threat detection and response.
5. Provide documentation and guidelines for secure cloud network management.
6. Establish data backup, disaster recovery, and failover mechanisms to ensure data continuity.
7. Achieve scalable architecture that maintains security while accommodating growth.

Project Summary

This project will involve design, implementation, and deployment of a Secure Cloud Network Architecture for Multi-Tier Applications by addressing the challenges of data security, network complexity, scalability, and lack of standardization. The project will provide a comprehensive solution that combines advanced encryption, Identity and Access Management (IAM), network segmentation, IDPS, data backup, and automation to ensure the security and scalability of multi-tier applications in a cloud environment.

Step 1: Define Service Offering

1.1. Scope and Features:

- The platform will offer automated deployment, scalability, monitoring, and security.

1.2. Service Tiers:

- Plan different service tiers (e.g., basic, advanced) with varying resource allocations and features.

Step 2: Set Up AWS Infrastructure

2.1. Multi-Tier Architecture:

- Design a multi-tier architecture with web, application, and database tiers.

- Use Amazon EC2 instances, RDS databases, and other AWS services as needed.

2.2. Network Configuration:

- Set up Virtual Private Cloud (VPC) with multiple subnets for each tier.

- Configure security groups to control traffic flow.

Step 3: Security and Compliance

3.1. IAM and Access Control:

- Implement IAM roles and policies to ensure secure access management for customers.

3.2. Encryption:

- Enable encryption at rest and in transit for data stored in the PaaS infrastructure.

Step 4: Monitoring and Analytics

4.1. CloudWatch Integration:

- Implement CloudWatch for monitoring and set up alarms to proactively manage resource utilization.

4.2. Log Aggregation:

- Set up AWS CloudTrail and Amazon CloudWatch Logs for centralized log aggregation.

Step 5: Load Balancing and Scalability

5.1. Load Balancing:

- Integrate Amazon Elastic Load Balancing to distribute traffic across instances.

5.2. Auto Scaling:

- Configure Auto Scaling groups to automatically adjust resources based on demand.

Step 6: Data Management and Backup

6.1. Database Management:

- Offer managed database services like Amazon RDS for easy database provisioning.

6.2. Automated Backups:

- Set up automated backups and snapshots for databases to ensure data integrity.

Step 7: Customer Onboarding and Management

7.1. Customer Dashboard:

- Develop a user-friendly dashboard for customers to manage their PaaS resources.

7.2. Billing and Cost Tracking:

- Integrate AWS Budgets and Cost Explorer to help customers track their service costs.

Step 8: Support and Documentation

8.1. Technical Support:

- Establish a support system to assist customers with technical issues and inquiries.

8.2. Documentation:

- Provide comprehensive documentation and tutorials to guide customers through using your PaaS.

Step 9: Customer Feedback

9.1. Feedback Collection and Iteration:

- Gather feedback from early customers to identify areas for improvement.

9.2. Continuous Improvement:

- Iteratively enhance your PaaS offering based on customer feedback and market trends.

Future Scope: Marketing and Launch

- **Branding and Website:** Design a website that promotes your PaaS service and highlights its features.
- **Marketing Campaign:** Launch a marketing campaign to attract potential customers to your PaaS offering with proper security and network implementation.

System Stakeholders

1. **Project Team:**
    i. Developers
    ii. Network Architects
    iii. Security Specialists
    iv. Compliance Experts
2. **Management:**
    i. Project Managers
    ii. IT Directors
    iii. CTOs
3. **End Users:**
    i. Enterprises
    ii. IT Administrators
4. **Cloud Service Provider (CSP):**
    i. Infrastructure Providers
    ii. Support Teams

Diagrams

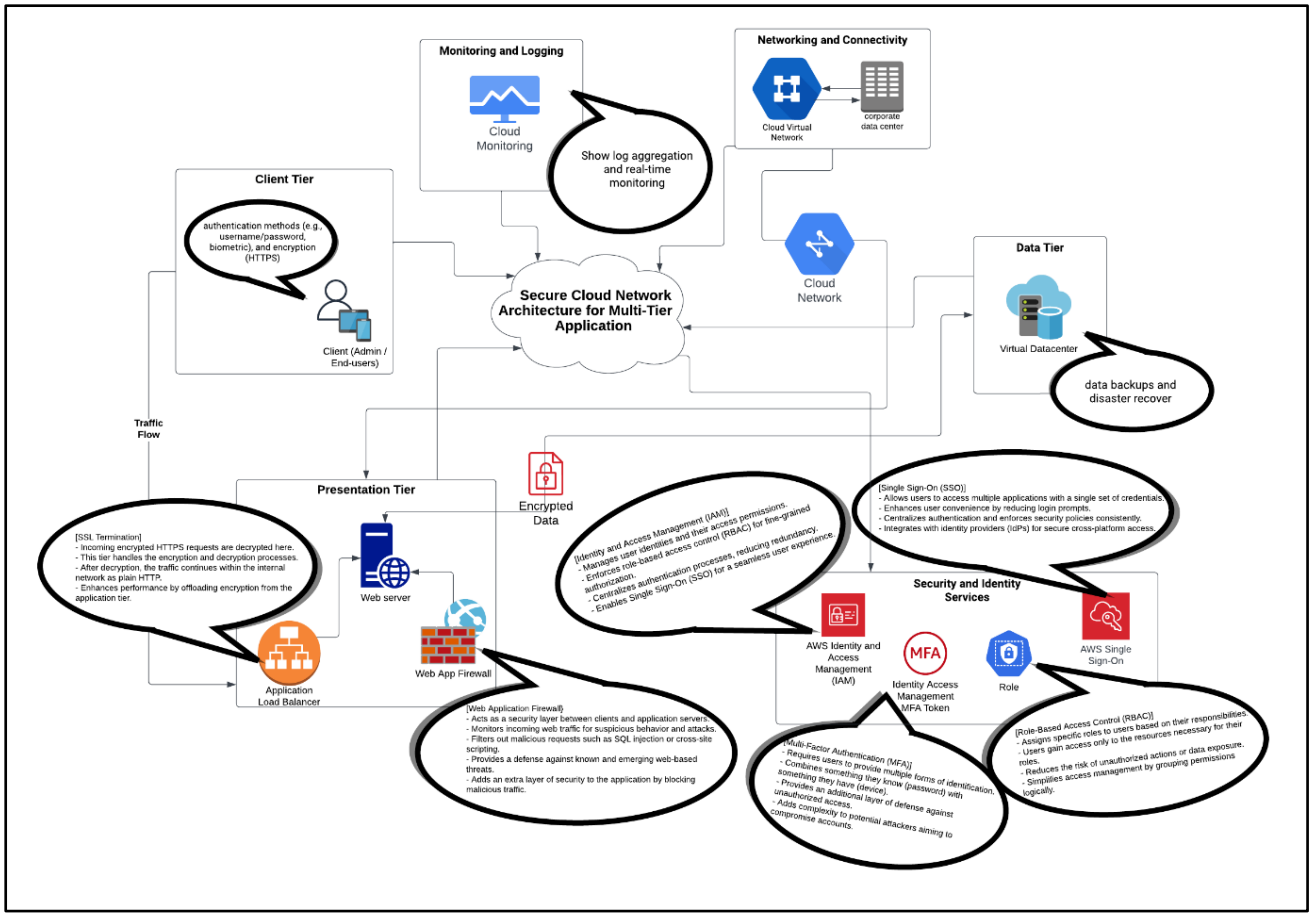

Figure 1: Rich Picture

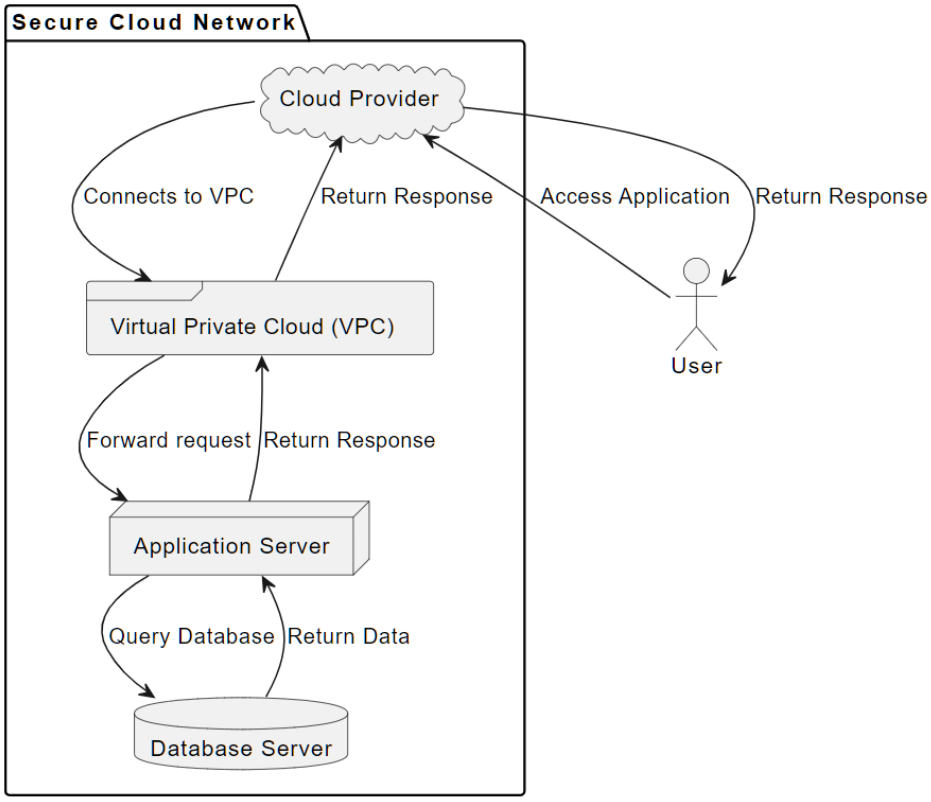

Figure 2: UML Diagram

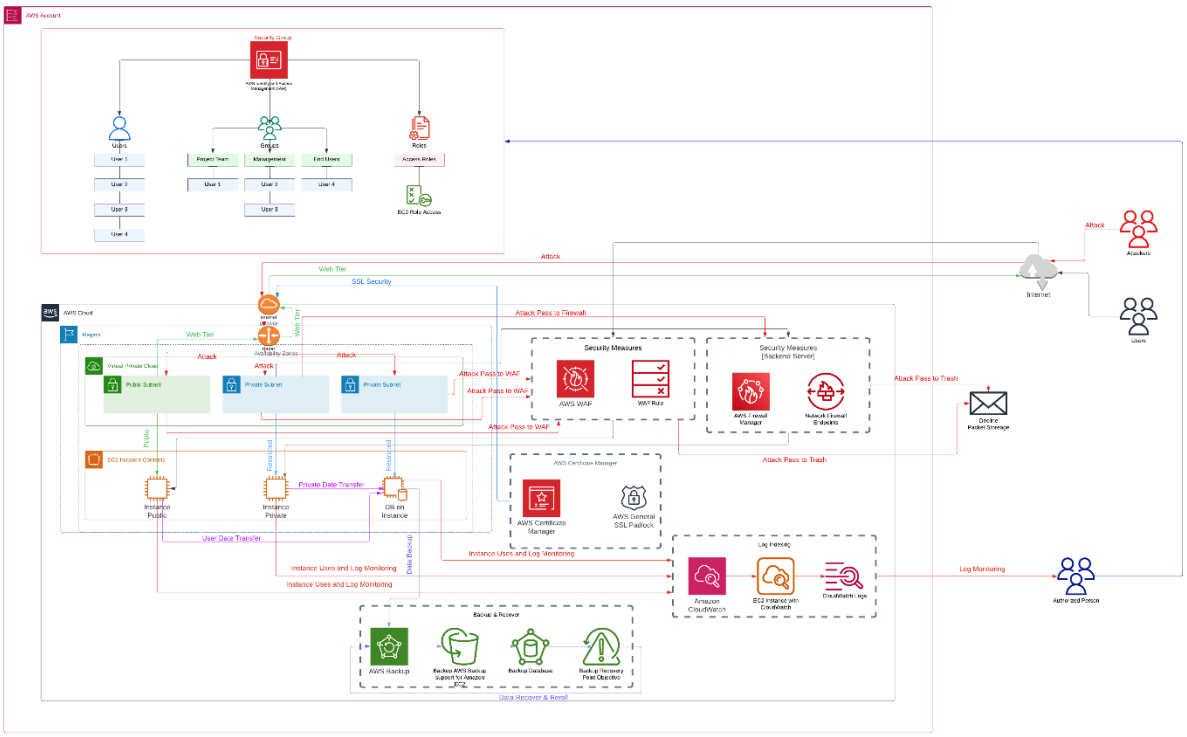

Figure 3: Data Flow Diagram (For one region)

Cloud Documentations

- **Infrastructure Documentation:** Detailed overview of the cloud infrastructure setup.
- **Security Guidelines:** Comprehensive documentation on security measures and best practices.
- **IAM Documentation:** User roles, permissions, and authentication protocols.
- **Network Configuration:** Network topology, segmentation strategies, and routing.
- **Scalability Documentation:** Guidelines for scaling the application without compromising security.
- **Compliance Reports:** Documentation showcasing automated compliance checks, detailing adherence to relevant regulations.
- **User Manuals:** Guides for end-users explaining how to interact with and manage the secure cloud network.

Security Features

- **Encryption:** Data at rest and in transit encryption using industry-standard algorithms.
- **IAM:** Role-based access control, multi-factor authentication, and single sign-on.
- **Network Segmentation:** Isolation of application tiers using virtual networks and firewalls.
- **IDPS:** Real-time monitoring and automated response to potential threats.
- **Automation:** Automated security protocols for threat detection and response.
- **Audit and Logging:** Comprehensive logging of activities for monitoring and forensics.