CCS6344 T2510 Database & Cloud Security Assignment 2: Secure Migration of a Traditional Application to AWS (Cloud Security) Group 39

ID	NAME	EMAIL
1211202024	NIKHILESH SHANDAVE DASS	1211202024@student.mmu.edu.my

Presentation Link : https://youtu.be/8cHTWN-1f9Q

Code Link (Github):
https://github.com/Nicky123rocks/CCS6344-T2510-Database-Cloud-Security-Assignment-2-Cloud-Security-Group-39.git

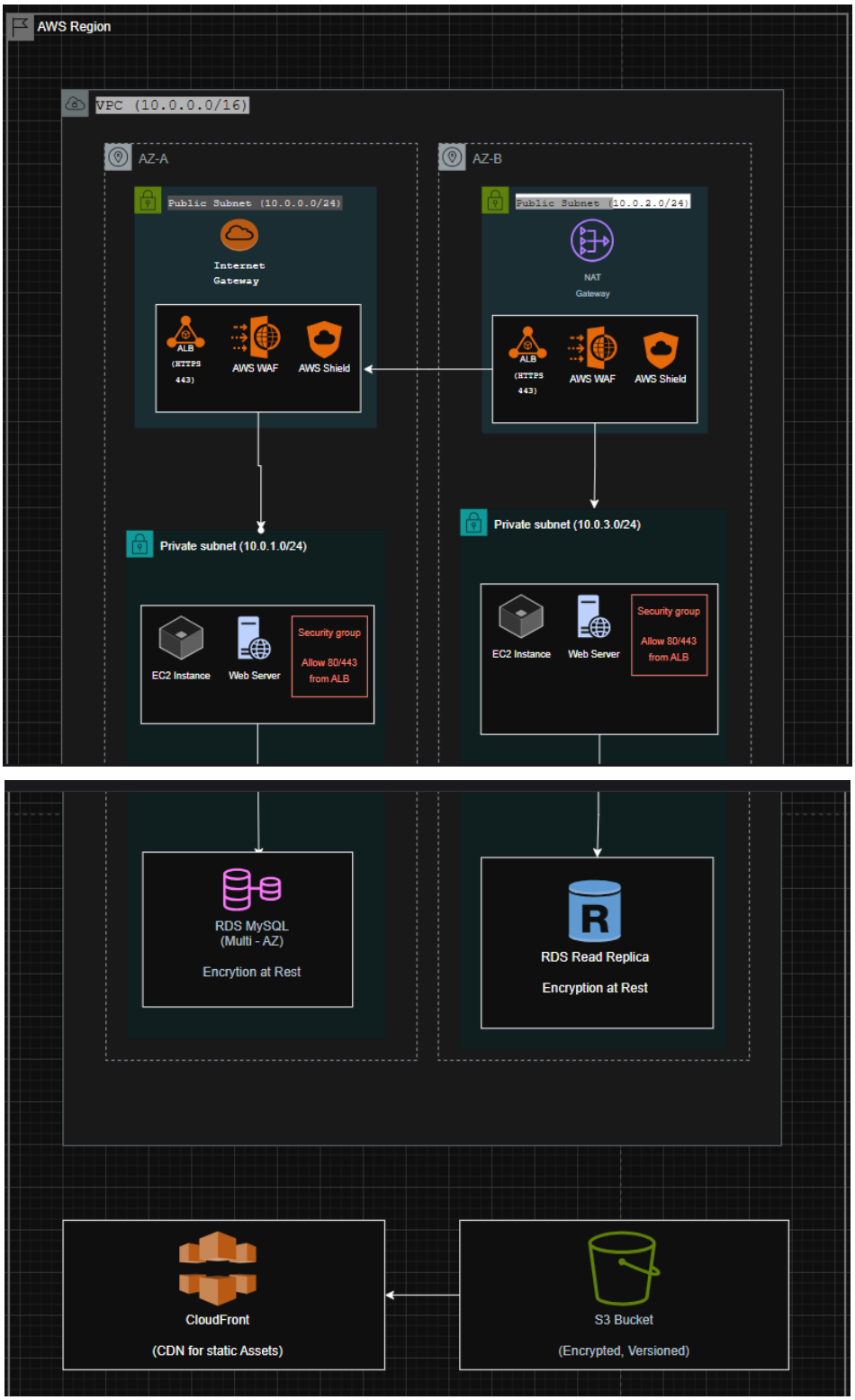
Security Risk Assessment & Migration Plan

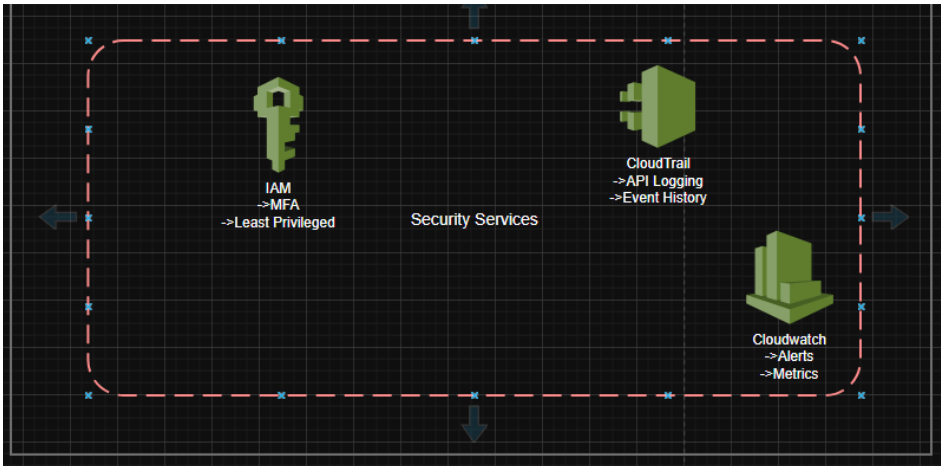
Security Vulnerabilities

No.	Vulnerability	Explanation
1.	Single Point Of Failure	If the single server fails, entire application and data become inaccessible
2.	Network Exposure	Without segmentation, databases and applications share a network, making it simple for attackers to switch between them
3.	No Encryption	Sensitive employee data is transmitted and stored in plain text
4.	Limited Access Control	Uses shared credentials; no granular user access policy
5.	No Monitoring or Logging	No audit logs, alerts, or breach detection mechanism
6.	No WAF (Web Application Firewall) or DDoS (Distributed Denial of Service) Protection	App is vulnerable to OWASP Top 10 attacks and denial-of-service
7.	Manual Backup & Recovery	No automated or off-site backup; risk of permanent data loss

Table 1 : Security Vulnerabilities

Proposed Architecture Diagram





AWS Architecture Diagram

Proposed AWS Architecture Description Diagram

Proposed AWS Architecture Description

1. **Core Infrastructure**
    - VPC Network: 10.0.0.0/16 spanning two Availability Zones (AZ-A and AZ-B)
        - Public Subnets:
            - 10.0.0.0/24 (AZ-A): Hosts Internet-facing resources
            - 10.0.2.0/24 (AZ-B): Contains NAT Gateway for outbound traffic
        - Private Subnets:
            - 10.0.1.0/24 (AZ-A) and 10.0.3.0/24 (AZ-B): Isolated workloads

2. **Compute & Networking**
    - Frontend Layer:
        - Application Load Balancer (ALB):
            - HTTPS termination (port 443)
            - Protected by AWS WAF (OWASP Core Rule Set)
            - Multi-AZ deployment for high availability
    - Backend Layer:
        - EC2 Instances (Apache/PHP):
            - Deployed in private subnets
            - Security Groups restrict traffic to ALB only (ports 80/443)
    - Database Layer:
        - Amazon RDS MySQL:
            - Multi-AZ deployment with encrypted storage
            - Read replica in AZ-B for failover

3. **Storage & Content Delivery**
    - Amazon S3:
        - Encrypted bucket (AES-256) with versioning
        - Stores static assets and database backups
    - CloudFront CDN:
        - Global distribution for S3-hosted content
        - Edge-optimized with TLS 1.2+

4. **Security Controls**
    - Network Security:
        - NACLs restrict traffic to required ports only
        - NAT Gateway enables controlled outbound access
    - Identity & Access:
        - IAM roles with least-privilege permissions
        - MFA enforcement for root/admin users
    - Monitoring:
        - CloudTrail for API activity logging
        - CloudWatch for metrics/alerts
        - VPC Flow Logs enabled

5. **High Availability Design**
    - All critical components deployed across two AZs
    - ALB routes traffic to healthy EC2 instances
    - RDS automatic failover to standby replica

6. **Encryption**
    - In Transit: TLS for ALB and CloudFront
    - At Rest:
        - RDS storage encryption (AWS KMS)
        - S3 server-side encryption

Main benefits

- Improved security through network isolation and encryption
- High availability with multi-AZ deployment
- Scalability via ALB and auto-scaling
- Reduced latency with CloudFront CDN

Security Migration Strategy

Risk	AWS Service	Migration Strategy
Single Point Of Failure	Application Load Balancer + EC2 Auto Scaling	Deploys multiple EC2 instances behind Application Load Balancer
Network Exposure	VPC + Private Subnets	Database resides in private subnets, unreachable from the internet
No Encryption	SSL/TLS + RDS Encryption	Use HTTPS via the Application Load Balancer, and also enable RDS Encryption
Limited Access Control	IAM + MFA	IAM roles to control EC2 Access, MFA for the IAM users
No Monitoring or Logging	CloudTrail + CloudWatch	Logs all Application Programming Interface, and also generate alerts on anomalies.
No WAF (Web Application Firewall) or DDoS (Distributed Denial of Service) Protection	AWS WAF	Blocks SQL injection, Cross-site Scripting, and DDoS
Manual Backup & Recovery	RDS Auto Backup + S3 Storage	Enables auto Database snapshot and version of object.

Table 2 : Security Migration Strategy

The End