Assignment 3

Design and Implementation of a Secure Cloud Application Architecture with Automated Threat Modeling and Risk Mitigation

Assignment Type: Design & Implementation

Problem Statement

Modern cloud applications are increasingly exposed to security threats due to their distributed and internet-facing nature. This assignment focuses on designing and implementing a secure cloud application architecture that integrates automated threat modeling, risk assessment, and mitigation mechanisms.

Objectives

- Design a secure cloud application architecture
- Perform automated threat modeling and risk analysis
- Implement automated threat detection and mitigation
- Evaluate system resilience under simulated attacks

System Requirements

The system must consist of the following components:
1. Client
2. API Gateway / Reverse Proxy
3. Application Server(s)
4. Data Storage Service
5. Security Monitoring and Logging Module

Tasks

Task 1: Secure Cloud Architecture Design

Design a secure architecture highlighting trust boundaries, data flow paths, and security enforcement points. Secure communication between components must be implemented.

Task 2: Authentication and Authorization

Implement token-based authentication and role-based access control. Logs must record successful and failed access attempts.

Task 3: Automated Threat Modeling

Apply a formal threat modeling methodology to identify threats and assess risks. Simulate multiple attack scenarios such as brute-force attacks and denial-of-service.

Task 4: Automated Risk Mitigation

Implement automated mitigation mechanisms including rate limiting, IP blocking, and account lockout. Mitigation actions must trigger automatically without manual intervention.

Task 5: Resilience and Recovery Evaluation

Evaluate system behavior under attack and partial service failure. Measure detection time, mitigation time, and system availability.

Logging and Evidence

Submit logs capturing authentication events, detected threats, mitigation actions, and recovery behavior. Screenshots must be provided as execution evidence.

Submission Requirements

```
Assignment3/
├── source_code/
│   ├── client/
│   ├── api_gateway/
│   ├── application_server/
│   ├── security_modules/
│   ├── monitoring/
│   └── README.md
├── diagrams/
│   └── architecture.png
├── logs/
│   ├── auth.log
│   ├── threats.log
│   └── mitigation.log
├── screenshots/
│   └── attack_scenario.png
└── report/
    └── Assignment3_Report.pdf
```