Mô hình UML Quản lý An toàn Thông tin cho Mobifone

II. Thiết kế các mô hình UML

1. Use Case Diagram

Các tác nhân:

- Khách hàng: Đăng nhập, cập nhật thông tin, khiếu nại bảo mật.
- Nhân viên CSKH: Hỗ trợ khách hàng, cập nhật thông tin bảo mật.
- Quản trị viên bảo mật: Quản lý tài khoản nhân viên, giám sát truy cập, xử lý sự kiện bảo mật.
- Hệ thống bảo mật: Phát hiện bất thường, gửi cảnh báo bảo mật.

Các Use Case chính:

- Đăng nhập hệ thống: Sử dụng xác thực 2 bước.
- Phân quyền truy cập: Nhân viên chỉ được truy cập thông tin theo vai trò.
- Giám sát truy cập bất thường: Hệ thống ghi log và thông báo khi có truy cập trái phép.
- Bảo vệ thông tin khách hàng: Mã hóa dữ liệu quan trọng.
- Xử lý khiếu nại bảo mật: Nhân viên CSKH tiếp nhận và xử lý khiếu nại liên quan đến rò rỉ dữ liệu.

2. Class Diagram

Các lớp chính:

1. **User**
    - id
    - username
    - password
    - role
    - email
    - phone

    - login()
    - updateInfo()
2. **Admin** (Kế thừa từ User)
    - manageRoles()
    - monitorSecurity()
3. **Customer** (Kế thừa từ User)
    - reportSecurityIssue()
4. **SecurityEvent**
    - eventID
    - userID
    - type
    - timestamp
    - status
    - detectAnomaly()
5. **AccessLog**
    - logID
    - userID
    - action
    - timestamp
    - IPAddress
    - recordActivity()

Mối quan hệ:

- User có thể là Admin hoặc Customer.
- Admin có thể quản lý quyền của Customer.
- SecurityEvent được tạo khi phát hiện hành vi bất thường từ User.
- AccessLog ghi nhận mọi thao tác của User.

3. Sequence Diagram

Tình huống 1: Đăng nhập hệ thống

1. Khách hàng nhập thông tin đăng nhập.
2. Hệ thống xác thực tài khoản và kiểm tra OTP.
3. Nếu hợp lệ, khách hàng được cấp quyền truy cập.

Tình huống 2: Phát hiện truy cập bất thường

1. Người dùng cố gắng đăng nhập từ một thiết bị lạ.
2. Hệ thống bảo mật phát hiện IP bất thường.
3. Hệ thống gửi cảnh báo qua email.

4. Entity-Relationship Diagram (ERD)

Các bảng dữ liệu chính:

1. **User** (userID, username, passwordHash, roleID, email, phone, lastLogin)
    - Khóa chính: userID
    - Khóa ngoại: roleID
2. **Role** (roleID, roleName, permissions)
    - Khóa chính: roleID
3. **SecurityEvent** (eventID, userID, eventType, timestamp, status)
    - Khóa chính: eventID
    - Khóa ngoại: userID
4. **AccessLog** (logID, userID, action, timestamp, IPAddress)
    - Khóa chính: logID
    - Khóa ngoại: userID

Quan hệ giữa các bảng:

- User có một Role, nhưng Role có thể liên kết với nhiều User.
- User có thể có nhiều SecurityEvent ghi nhận các sự kiện bất thường.
- User có nhiều AccessLog để ghi lại hoạt động đăng nhập.

Ghi chú

Hệ thống đảm bảo:

- Dữ liệu được mã hóa trước khi lưu trữ.
- Mọi sự kiện đều được ghi nhật ký và theo dõi.
- Chỉ người dùng có quyền mới được phép truy cập các chức năng quan trọng.

Mô hình trên giúp đảm bảo tính toàn vẹn, bảo mật và tính sẵn sàng của thông tin khách hàng trong hệ thống Mobifone.