**King Fahd University of Petroleum & Minerals**

**Department of Information and Computer Science**



**SWE 445: Secure Software Development**

**Project: Phase 2**

**Team No.**: 6

**Team Members**:

|  |  |
| --- | --- |
| **Name** | **ID** |
| OMAR MOHAMMED SAIKHAN | 201928330 |
| MOHAMMED ALOTAIBI | 201932090 |
| MAHMOUD ALMARHOON | 202015020 |
| ESSA ALMUTAWA | 201959470 |



1. **User Interface Design: High-fidelity prototypes for three mitigation use cases and three related use cases.**
2. **Login/SignUp (use case)**

A screenshot of a login page

AI-generated content may be incorrect.

1. **Login/SignUp (mitigation)**

**Note: the mitigation by**

**authentication by Google Firebase**

**when the user try login 3 times block will happen**

**A screenshot of a login screen

AI-generated content may be incorrect.**

1. **XXX (use case)**
2. **XXX(mitigation)**
3. **ZZZ(use case)**
4. **ZZZ(mitigation)**
5. **Database Design: Entity-Relationship Diagram (ERD) highlighting primary keys, foreign keys, and alternative keys for selected use cases.**

**A diagram of a company

AI-generated content may be incorrect.**

1. **Describe which design principle will be implemented (choose at least 2 design principles)**

**Principle of Least Privilege (POLP)**  
**Description:**  
The system follows the Principle of Least Privilege to ensure that each user or system component has only the permissions necessary to perform their specific tasks. This minimizes the potential for unauthorized access or misuse of sensitive data.

**Implementation in the Project:**

* **Role-Based Access Control (RBAC):**
  + Patients can only view and manage their own profiles, medical history, and appointments.
  + Doctors can view and update patient medical records but cannot modify user roles or access system settings.
  + Admins can manage users and system configurations but cannot edit medical records.
* This ensures that users only interact with the data and functionalities required for their roles, reducing the risk of errors or security breaches.

**Defense in Depth**  
**Description:**  
The system employs multiple layers of security controls to protect data and ensure system resilience against attacks. Even if one security mechanism fails, other measures continue to safeguard the system.

**Implementation in the Project:**

* **Secure Authentication Using Firebase:**
  + Login and sign-up credentials are encrypted using Firebase Authentication, which applies robust hashing and salting techniques to protect user passwords.
* **Account Lockout After Multiple Failed Login Attempts:**
  + Users are blocked after three consecutive failed login attempts. To unblock, users must verify their identity through email or OTP verification.
* **Encryption for Sensitive Data:**
  + Sensitive data, such as medical records, is encrypted at rest (in the database using AES-256) and in transit (using HTTPS).
* **Activity Monitoring and Logging:**
  + All user activities, including failed login attempts, are logged to detect and respond to suspicious behaviors. Alerts are sent to admins for repeated suspicious activity.