**King Fahd University of Petroleum & Minerals**

**Department of Information and Computer Science**



**SWE 445: Secure Software Development**

**Project: Phase 1**

**Team No.**: 6

**Team Members**:

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



**a) requirements for each of the six core security concepts** in the context of the **As-Shifa Secure Healthcare Management System**.

**1. Confidentiality**

**Objective**: Ensure that patient data is only accessible to authorized individuals.

**Requirements**:

* Patient records (e.g., medical history, prescriptions) must be encrypted both in transit and at rest.
* Access to sensitive data (e.g., medical records) must be restricted to authorized personnel (e.g., doctors, nurses) based on their roles.
* Patients must be able to control who can access their medical information (e.g., sharing with specific doctors or facilities).
* Unique patient IDs must be generated to ensure secure identification and prevent unauthorized access.
* The system must comply with data privacy regulations (e.g., HIPAA, GDPR) to protect patient confidentiality.

**2. Integrity**

**Objective**: Ensure that patient data is accurate and not tampered with.

**Requirements**:

* All data entries (e.g., medical history, prescriptions) must be validated to prevent incorrect or malicious input.
* Any changes to patient records must be logged, and the system must ensure that only authorized users can modify data.
* The system must use checksums or digital signatures to detect unauthorized modifications to data.
* Patients and doctors must be able to verify the accuracy of medical records during consultations.

**3. Availability**

**Objective**: Ensure that the system and data are accessible when needed.

**Requirements**:

* The system must have high uptime (e.g., 99.9% availability) to ensure it is always accessible to patients and healthcare providers.
* Backup and disaster recovery mechanisms must be in place to restore data in case of system failure.
* The system must be scalable to handle increased load during peak times (e.g., flu season).
* Patients and doctors must be able to access the system from multiple devices (e.g., desktop, mobile) without interruption.

**4. Authentication**

**Objective**: Verify the identity of users accessing the system.

**Requirements**:

* All users (e.g., patients, doctors, insurance providers) must authenticate themselves using secure methods (e.g., username/password, two-factor authentication).
* Passwords must meet complexity requirements (e.g., minimum length, special characters) and be stored securely (e.g., hashed and salted).
* Patients and doctors must be able to reset their passwords securely in case they forget them.
* The system must prevent brute-force attacks by locking accounts after a certain number of failed login attempts.

**5. Authorization**

**Objective**: Ensure that users have the appropriate permissions to access specific data or perform certain actions.

**Requirements**:

* Role-based access control (RBAC) must be implemented to restrict access based on user roles (e.g., patients can only view their own records, doctors can view and update records).
* Patients must be able to grant or revoke access to their medical records for specific healthcare providers.
* Insurance providers should only have access to the data required for processing claims (e.g., treatment details, costs).
* The system must enforce least privilege, ensuring users only have access to the data and functions necessary for their role.

**6. Accountability (Logging/Auditing)**

**Objective**: Keep track of who accessed or modified data and when.

**Requirements**:

* All access to patient records (e.g., viewing, updating) must be logged, including the user’s ID, timestamp, and action performed.
* The system must generate audit logs that can be reviewed to detect unauthorized access or suspicious activity.
* Patients must be able to request a report of who accessed their medical records and for what purpose.

**b) Use case, Misuse cases, and Actors of AS-Shifa system.**

**Actors:**

1. **Patient**
2. **Doctor**
3. **Insurance Provider**
4. **System Administrator**

**Use Cases:**

1. **Patient**:
   * Register
   * Log In
   * View Medical Records
   * Schedule Appointment
   * Share Medical Information
2. **Doctor**:
   * Log In
   * View Patient Records
   * Update Patient Records
   * Prescribe Medication
3. **Insurance Provider**:
   * Verify Insurance
   * Process Claims
4. **System Administrator**:
   * Manage Accounts
   * Monitor Logs

**Misuse Case Actors:**

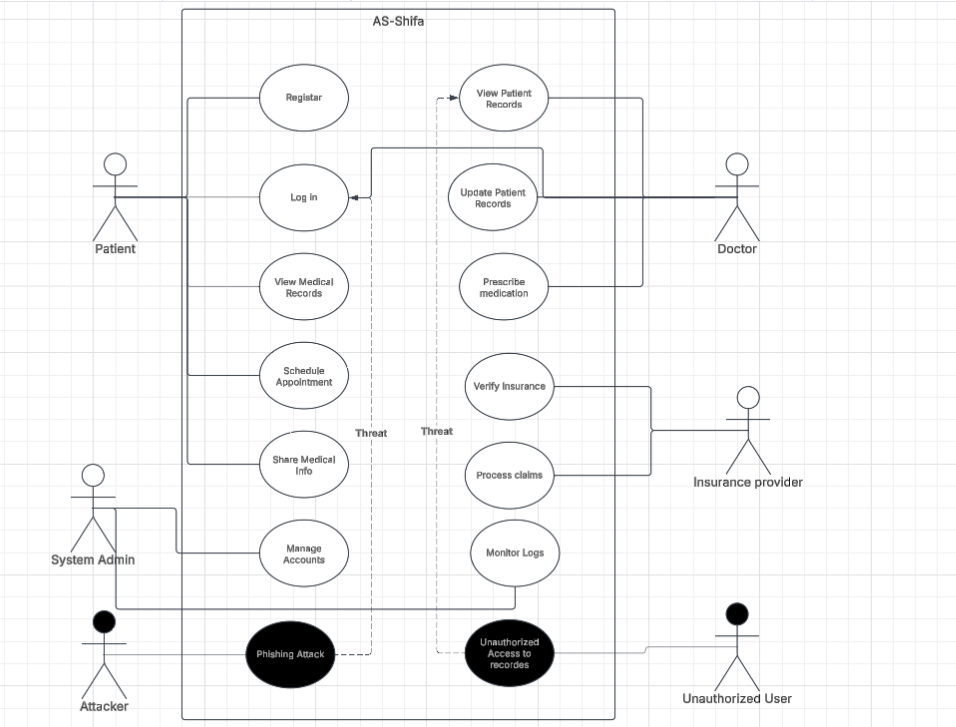
**Unauthorized User:**

* **Misuse Case 1**: **Unauthorized Access to Patient Records**
  + **Threatened Use Case**: **View Medical Records** (Patient/Doctor/Nurse)
  + **Explanation**: An unauthorized user could gain access to sensitive patient records, violating confidentiality.

**Attacker:**

* **Misuse Case 2**: **Phishing Attack**
  + **Threatened Use Case**: **Log In to the System** (Patient/Doctor/Nurse/System Admin)
  + **Explanation**: A phishing attacker could trick users into revealing their login credentials, compromising their accounts.

**The Use case and Misuse case diagram so far (before mitigation):**



**(c) Add use cases (mitigation use cases) to mitigate misuse cases identified in section (b).**

**A diagram of a company

AI-generated content may be incorrect.**

**(d) Write a description for all identified use cases/misuse cases, etc.**

**Use Cases Description:**

|  |  |
| --- | --- |
| UC-01: Register | |
| Description: | Allow a patient to create an account in the system. |
| Actors: | Patient. |
| Main Flow: | 1. The patient provides personal details and submits the registration request. 2. The system verifies the provided information. 3. If valid, the system creates a new patient account. 4. The patient receives a confirmation notification. |
| Alternative(s): | If the details are invalid, the system prompts the patient to re-enter information. |

|  |  |
| --- | --- |
| UC-02: Log In | |
| Description: | Allows an authenticated user to access the system. |
| Actors: | Patient, Doctor, Insurance Provider, System Admin. |
| Main Flow: | 1. The user enters credentials. 2. The system validates the credentials. 3. If valid, the user gains access to the system. |
| Alternative(s): | If credentials are incorrect, the system displays an error and prompts retry. |

|  |  |
| --- | --- |
| UC-03: View Medical Records | |
| Description: | Enables a patient to view their medical history. |
| Actors: | Patient. |
| Main Flow: | 1. The patient logs in. 2. The patient navigates to the medical records section. 3. The system retrieves and displays the patient’s records. |
| Alternative(s): | If records are unavailable, the system notifies the patient. |

|  |  |
| --- | --- |
| UC-04: Schedule Appointment | |
| Description: | Allows patients to book a medical appointment. |
| Actors: | Patient. |
| Main Flow: | 1. The patient logs in and navigates to the appointment section. 2. The patient selects an available slot. 3. The system confirms the appointment. |
| Alternative(s): | If no slots are available, the patient receives a notification. |

|  |  |
| --- | --- |
| UC-05: Share Medical Information | |
| Description: | Enables a patient to share their medical history with authorized parties. |
| Actors: | Patient. |
| Main Flow: | 1. The patient selects the records to share. 2. The system requests confirmation. 3. If confirmed, the system grants access to the recipient. |
| Alternative(s): | If unauthorized sharing is attempted, the system denies the request. |

|  |  |
| --- | --- |
| UC-06: View Patient Records | |
| Description: | Enables doctors to access patient medical records. |
| Actors: | doctor. |
| Main Flow: | 1. The doctor logs in. 2. The doctor searches for a patient’s records. 3. The system retrieves and displays the records. |
| Alternative(s): | If the patient’s records are restricted, access is denied. |

|  |  |
| --- | --- |
| UC-07: Update Patient Records | |
| Description: | Allows doctors to modify patient records with new medical information. |
| Actors: | Doctor. |
| Main Flow: | 1. The doctor selects a patient’s profile. 2. The doctor updates the records. 3. The system saves changes. |
| Alternative(s): | If unauthorized modifications are attempted, the system logs the action. |

|  |  |
| --- | --- |
| UC-08: Prescribe Medication | |
| Description: | Allows doctors to issue prescriptions to patients. |
| Actors: | Doctor. |
| Main Flow: | 1. The doctor selects a patient’s profile. 2. The doctor enters prescription details. 3. The system stores the prescription. 4. The patient receives a notification. |
| Alternative(s): | If prescription data is incomplete, the system prompts for completion. |

|  |  |
| --- | --- |
| UC-09: Verify Insurance | |
| Description: | Enables the system to verify a patient’s insurance status. |
| Actors: | Insurance provider. |
| Main Flow: | 1. The insurance provider receives a verification request. 2. The system checks policy details. 3. If valid, verification is approved. |
| Alternative(s): | If the insurance is expired, the request is rejected. |

|  |  |
| --- | --- |
| UC-10: Process Claims | |
| Description: | Handles insurance claims submitted by patients. |
| Actors: | Insurance provider. |
| Main Flow: | 1. The patient submits an insurance claim. 2. The provider reviews and processes the claim. 3. The system notifies the patient of the decision. |
| Alternative(s): | If fraud is suspected, the claim is flagged. |

|  |  |
| --- | --- |
| UC-11: Manage Accounts | |
| Description: | Allows the system administrator to manage user accounts. |
| Actors: | System admin. |
| Main Flow: | 1. The admin logs in. 2. The admin adds, modifies, or deletes user accounts. 3. The system updates records accordingly. |
| Alternative(s): | If unauthorized account actions are attempted, they are logged. |

|  |  |
| --- | --- |
| UC-12: Monitor Logs | |
| Description: | Enables administrators to track system activity for security purposes. |
| Actors: | System admin. |
| Main Flow: | 1. The admin logs in. 2. The admin reviews system logs. 3. Any suspicious activity is flagged. |
| Alternative(s): | If logs show security breaches, alerts are generated. |

**Misuse Cases Description:**

|  |  |
| --- | --- |
| UC-13: Unauthorized Access to Records | |
| Description: | An unauthorized user attempts to access patient records. |
| Actors: | Unauthorized user. |
| Main Flow: | 1. The attacker attempts to log in using stolen credentials. 2. The system detects multiple failed attempts. 3. The system locks the account and alerts the admin. |
| Alternative(s): | If an unauthorized user gains access, the system logs the activity for review. |
| Mitigation Points | * Implement multi-factor authentication. * Log and monitor failed login attempts. |

|  |  |
| --- | --- |
| UC-14: Phishing Attack | |
| Description: | An attacker attempts to obtain user credentials through phishing. |
| Actors: | Attacker. |
| Main Flow: | 1. The attacker sends fraudulent emails to users. 2. A user unknowingly enters credentials into a fake site. 3. The attacker gains unauthorized access. |
| Alternative(s): | If the attack is detected, the system alerts users. |
| Mitigation Points | * Educate users on phishing risks. * Implement email filtering and link verification systems. |