SUBSYSTEM NAME: *[***Case Management***]*

GROUP NAMES:

1. *Mohammed Al-Mughalles*
2. *Nehal Al-Odaini*

Table of Contents

Threat Model

In this document, we will provide a threat modeling about [Case Management].

1 Scope

In this section, we will To improve how judicial cases are managed with an integrated system that helps to follow procedures and access information.

1.1 Information

APPLICATION NAME	Case Management
APPLICATION VERSION	Judicial Case Management System
DESCRIPTION	an integrated system whose purpose is to manage the cases in the juristic system. Easy to use interface for recording, following up cases, managing legal docs and Communicating amongst the parties concerned.
DOCUMENT OWNER	Mohammed Alqmase
PARTICIPANTS	*1. Majed Bagash* *2. Mohammed Al-Mugalees* *3. Ahmed Al-Hakeemy* *4. Ramzi Al-Qubaty* *5. Nehal Al-Odaini*
REVIEWER	Fahd Al-Mughalles

1.2 Dependencies

ID	EXTERNAL DEPENDENCIES DESCRIPTION
1	**Case Database:** Storage of all case and stakeholder data
2	**API:** Integration with other systems such as criminal records
3	**document management system:** Storage and management of legal documents associated with cases
4	**Authentication system:** Provide an additional level of security by confirming users' identity

1.3 Entry Points

ID	NAME	DESCRIPTION	TRUST LEVELS
1	**user interface**	The interactive interface used by lawyers and judges to manage cases.	high
2	**API**	API for integration with external systems such as court records.	medium
3	**mobile app**	A dedicated application for users to access information and manage issues.	high
4	**Safe Access Portal**	Authentication and identity verification system for users.	high

1.4 Exit Points

ID	NAME	DESCRIPTION	TRUST LEVELS
1	**Judges' Reports**	Reports are established to follow up and manage the status of cases.	high
2	**email notifications**	Notifications sent to users regarding issue updates.	medium
3	**Export Interface**	The possibility of exporting data to other systems or formats.	medium
4	**Exit Interface**	The process of logging out of the system securely.	high

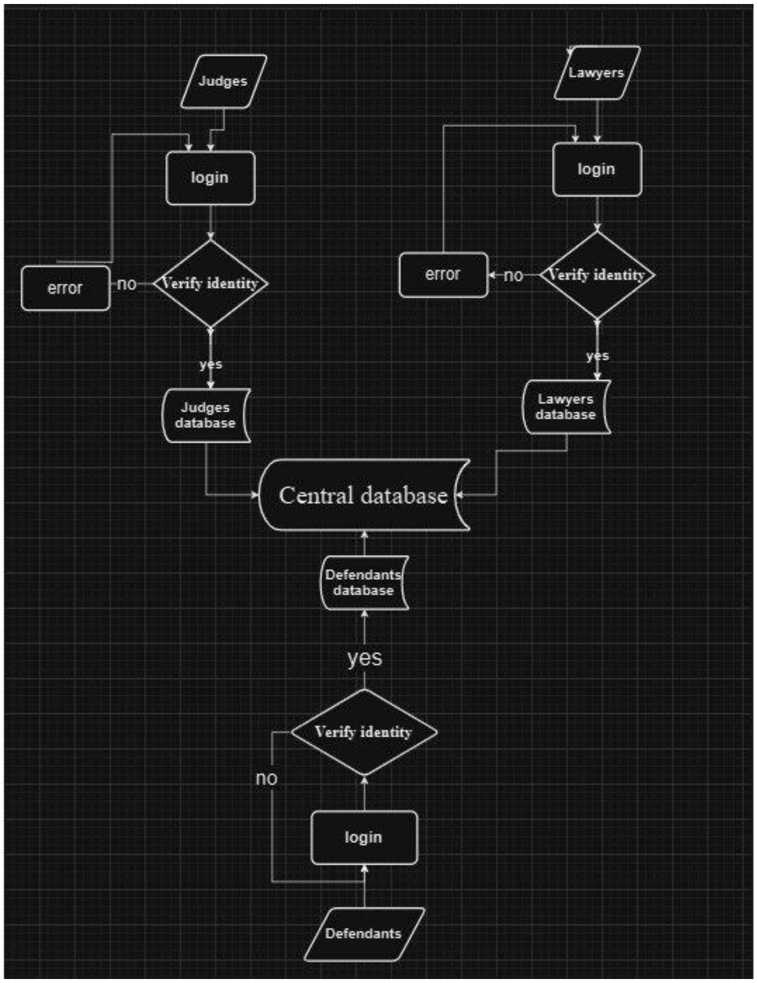
1.5 Assets

ID	NAME	DESCRIPTION	TRUST LEVELS
1	**Case Database**	A database containing all case information, stakeholders and documents.	high
2	**users' data**	Users' information such as entry data, roles, and personal information.	high
3	**legal documents**	all documents related to issues such as complaints, replies, and judgments.	high
4	**user interface**	The interface with which users interact to manage issues.	Medium

1.6 Trust Levels

ID	NAME	DESCRIPTION
1	**high-level**	Accredited users such as judges and lawyers with full access to sensitive data.
2	**intermediate level**	Support staff or staff of the system who need access to limited information.
3	**low-level**	Visitors or unregistered users who have access to general information only.
4	**special level**	Users with special roles such as investigators or experts who need specific access for certain purposes.

1.7 Data Flow Diagrams



2 Break

In this section, we will analyze the weaknesses of the case management system. To ensure maximum security of computer software or hardware, it is essential to know their vulnerabilities. Every vulnerability shall be assessed based on its impact, likelihood of occurrence and remedial measures

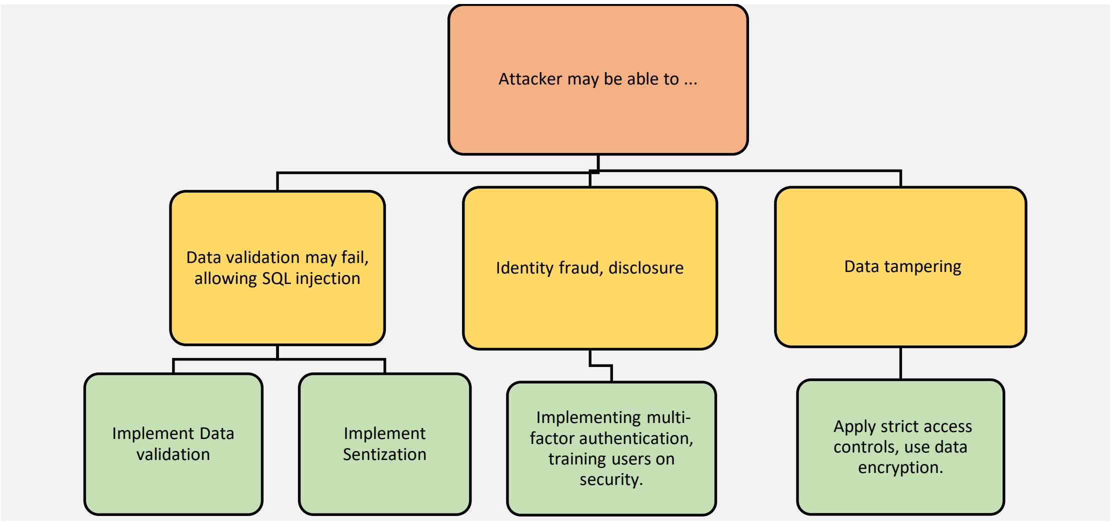
2.1 STRIDE Framework

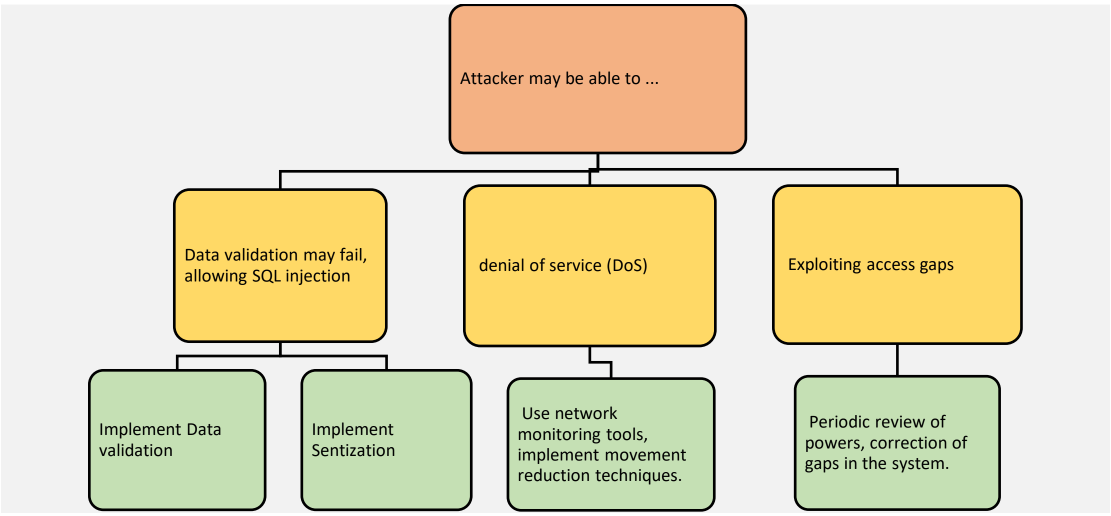
ID	THREATS TYPES	THREATS DESCRIPTION	SECURITY CONTROL TYPES
1	**Spoofing**	1. impersonate a user for unauthorized access. 2. Loss of data, violation of privacy.	Authentication
2	**Tampering**	1. Modify data or system settings unauthorized. 2. Impact on the integrity of information, loss of trust.	Integrity
3	**Repudiation**	1. Deny the user to do a certain job such as making a case. 2. Loss of records, inability to track procedures.	Non- Repudiation
4	**Information Disclosure**	1. Leak sensitive information to unauthorized parties. 2. Violation of privacy, legal damages.	Confidentiality
5	**Denial of Service**	1. Attacks aimed at making the system unavailable to legitimate users. 2. Loss of productivity, inability to access services.	Availability
6	**Elevation of Privileges**	1. Obtaining unauthorized higher powers. 2. Data violation, loss of control over the system.	Authorization

2.2 Threat Analysis

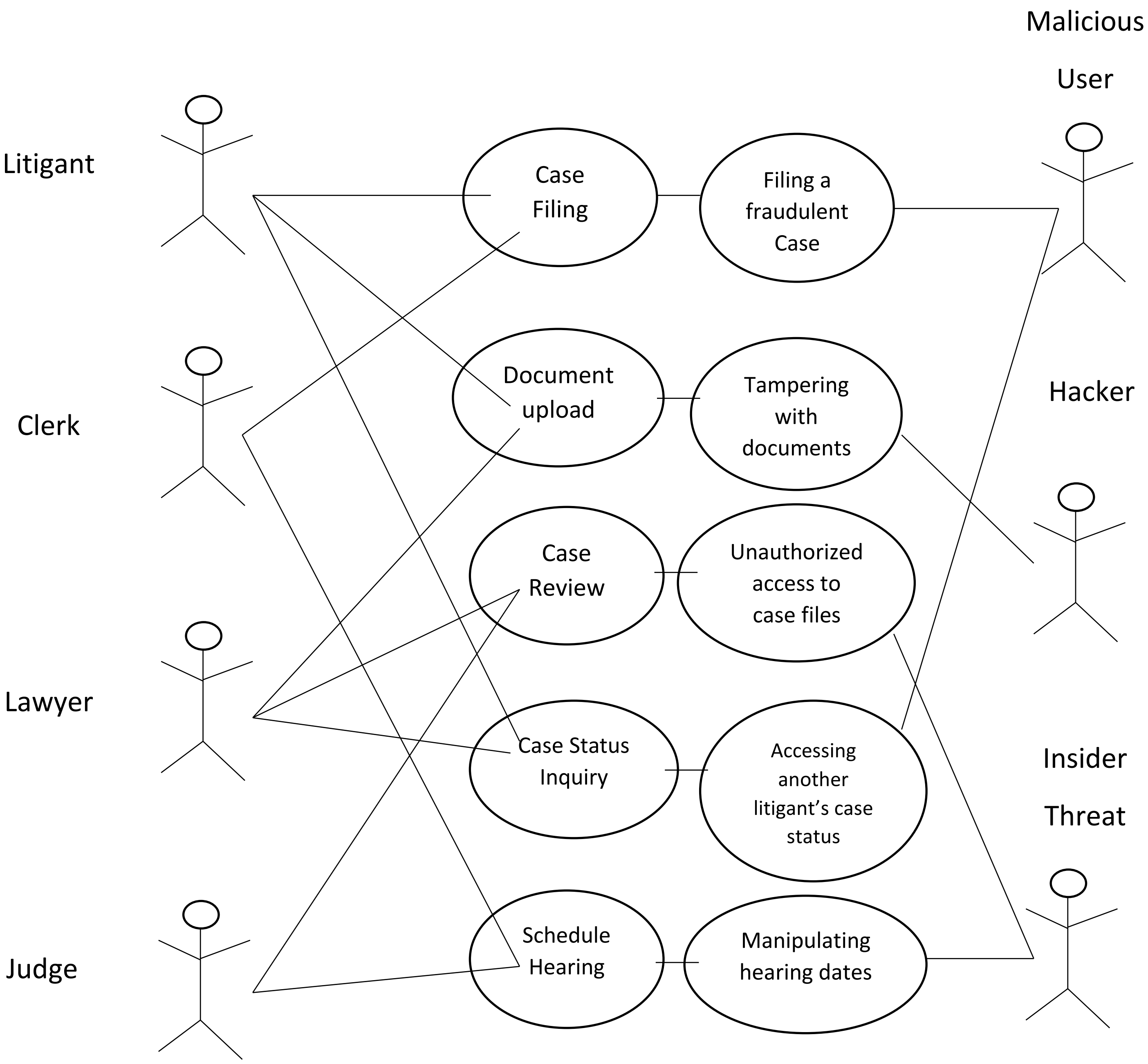
In this section, we will conduct a comprehensive threat analysis to identify, assess, and prioritize potential threats to the case management system. This analysis will help us understand the vulnerabilities within the system and the possible impacts of various threats.

2.2.1 Attack Trees


Attacker may be able to ...
Data validation may fail, allowing SQL injection
Identity fraud, disclosure
Data tampering
Implement Data validation
Implement Sentization
Implementing multi-factor authentication, training users on security.
Apply strict access controls, use data encryption.


Attacker may be able to ...
Data validation may fail, allowing SQL injection
denial of service (DoS)
Exploiting access gaps
Implement Data validation
Implement Sentization
Use network monitoring tools, implement movement reduction techniques.
Periodic review of powers, correction of gaps in the system.

2.2.2 Misuse Cases



2.2.3 Threat Description Table

THREAT ID	THREAT DESCRIPTION	THREATS TYPES
1	Fraudulent user identity to access case data	Spoofing
2	Disclosure of sensitive case information to unauthorized entities	Spoofing
3	Unauthorized modification of case statements	Tampering
4	Disruption of the system preventing access to judicial services	Tampering
5	Raise user powers to access sensitive data	Information Disclosure
6	Disclaimer of acts such as submitting cases or amending statements	Denial of Service

2.3 Ranking

In this section, we will Rank the identified threats by how serious and likely they might occur. By priority ranking this development in terms of gravity probability the mitigation steps can be directed towards the most impactful threats.

2.3.1 Delphi Ranking

THREAT ID	THREAT TITLE	MEMBER 1 RANK	MEMBER 2 RANK	MEMBER 3 RANK	AVERAGE RANK	FINAL CONSENSUS RANK	COMMENTS
1	**User Identity Fraud**	2	1	2	1.5	1	Very high threat
2	**disclosing sensitive information**	1	2	1	1.5	1	Requires strict safety procedures
3	**Amending case data**	3	3	3	3	3	Average risk
4	**disable the system**	1	2	1	1.5	1	Significant impact on operations
5	**User permissions *power***	2	3	2	2.5	2	Powers must be monitored
6	**Disclaimer**	3	3	3	3	3	less risky

2.3.2 Average Ranking

THREAT ID	THREAT TITLE	D	R	E	A	AVERAGE RANK	RISK LEVELS
1	**User Identity Fraud**					1.5	Very high
2	**reveal sensitive information**					1.5	Very high

3	**Modify case data**					3	medium
4	**disable the system**					1.5	Very high
5	**User permissions *power***					2.5	high
6	**Disclaimer**					3	low

2.3.3 Probability x Impact (P x I) Ranking

Threat ID	Threat Title	P probability	I Impact	Risk Score P x I	Rank
1	**User Identity Fraud**	4	5	20	1
2	**reveal sensitive information**	4	5	20	1
3	**Modify case data**	3	4	12	3
4	**disable the system**	4	5	20	1
5	**User permissions *power***	3	3	9	4
6	**Disclaimer**	2	2	4	6

Remarks:

PROBABILITY: Ranges from 1 (low) to 5 (high).

IMPACT: ranges from 1 (low) to 5 (high).

RISK SCORE: Calculated as follows: PROBABILITY × IMPACT.

3 Fix

In this section, we will outline the strategies and actions necessary to mitigate the identified threats to the case management system. Our goal is to implement effective fixes that reduce vulnerabilities and enhance the overall security posture of the system.

Threat ID	T#001
Threat Description	User identity fraud Attempt unauthorized access to the system using a false identity.
Threat targets	1. users' data 2. Case records
Attack techniques	1. phishing attack 2. Exploiting passwords 3. Use of identity manipulation tools
Security Impact	1. Loss of sensitive data 2. Destroy trust between users and the system 3. Negative impact on legal processes
Risk	very high
Safeguard controls to implement	1. Implementation of Role Based Access Control System (RBAC) 2. Multi-factor authentication application (MFA) 3. Monitoring and recording of suspicious activities

Threat ID	T#002
Threat Description	Leaking sensitive data from the system to unauthorized entities.
Threat targets	1. Case Information 2. customer details
Attack techniques	1. Gaps-exploiting attacks 2. unauthorized access 3. malware attacks
Security Impact	1.Loss of sensitive data 2. Legal implications 3. Destroy the reputation of the enterprise

RISK	high
SAFEGUARD CONTROLS TO IMPLEMENT	1. Encryption of sensitive data 2. Implement strict safety policies 3. Regular security audits

THREAT ID	T#003
THREAT DESCRIPTION	Unauthorized change or deletion of case statements.
THREAT TARGETS	1. Case records 2. Users' Information
ATTACK TECHNIQUES	1. Unauthorized access 2. Exploiting system gaps 3. Using data manipulation tools
SECURITY IMPACT	1. Negative impact on data integrity 2. Loss of trust in the system 3. Legal implications
RISK	high
SAFEGUARD CONTROLS TO IMPLEMENT	1. Implementation of regular data audits 2. Use of digital signature techniques 3. Application of accurate access control system

4 Verify

In this section, we will outline the processes and methods used to verify the effectiveness of the implemented fixes and ensure that the case management system is secure and functioning as intended. This includes reviewing documentation, testing the system, and validating the results.

4.1 Review Documentation

We will conduct a thorough review of all relevant documentation, including:

- **Security Policies**: Ensure that all security policies are updated and reflect the current practices.
- **User Access Logs**: Analyze logs to verify that access controls are being enforced appropriately.
- **Incident Reports**: Review past incidents to identify any recurring issues and ensure lessons learned are documented.

4.2 Test cases

We will develop and execute test cases to verify that the implemented fixes are effective. This will include:

- **Functional Tests**: Verify that all system functionalities are working as intended after the fixes.
- **Security Tests**: Conduct penetration testing and vulnerability assessments to identify any remaining weaknesses.
- **User Acceptance Testing (UAT)**: Involve end-users to validate that the system meets their needs and expectations.

4.3 Validation

Validation will involve confirming that the system meets all defined requirements and standards. This will include:

- **Compliance Checks**: Ensure that the system complies with relevant legal and regulatory requirements.
- **Performance Metrics**: Measure system performance against established benchmarks to ensure that it operates efficiently.
- **Feedback Mechanism**: Collect feedback from users to identify any issues or areas for improvement.