APPOINTMENT AND SCHEDULING MANAGEMENT INFORMATION SYSTEM

Essex
MSc CyberSecurity

1 Table of Contents

2 Objectives:

Queens medical centre is a clinic and servers as the first point of call for any resident within the catchment area, all the current doctor appointment are booked over the phone. The new appointment and scheduling management information system (ASMIS) at Queens medical center allows potential patients to schedule appointments online. This system will collect crucial patient information in order to schedule a doctor's visit. As a result of this technology, the patient's appointment scheduling experience will be improved.

3 Identification of the requirements:

- The ASMIS system to collect patient PII vital (personal identifiable information) information during the registration process.
- The ASMIS system should allow the returning patient to schedule and modify the existing appointments
- The receptionist/office staff should be able to manage appointments of the patient
- Secure patient personal and health information
- Host the application on on-premises datacenter
- Obscure the vital data and mask the data where necessary
- Secure communication between client and server
- Encrypt data in motion and data at rest
- Maintain least privilege

4 INTRODUCTION

Scope of this document to discuss the web-based appointment and scheduling management information system (ASMIS) system overview and its threat modeling.

ASMIS systems are used to manage patient health and personal records, which contain a wide range of data obtained from the various interactions patients have with medical professionals. The increasing acceptance of their use necessitates an increased focus on electronic health system security.

The following use case diagram shows how patient schedule the appointments.

ASMIS Use case Diagram:

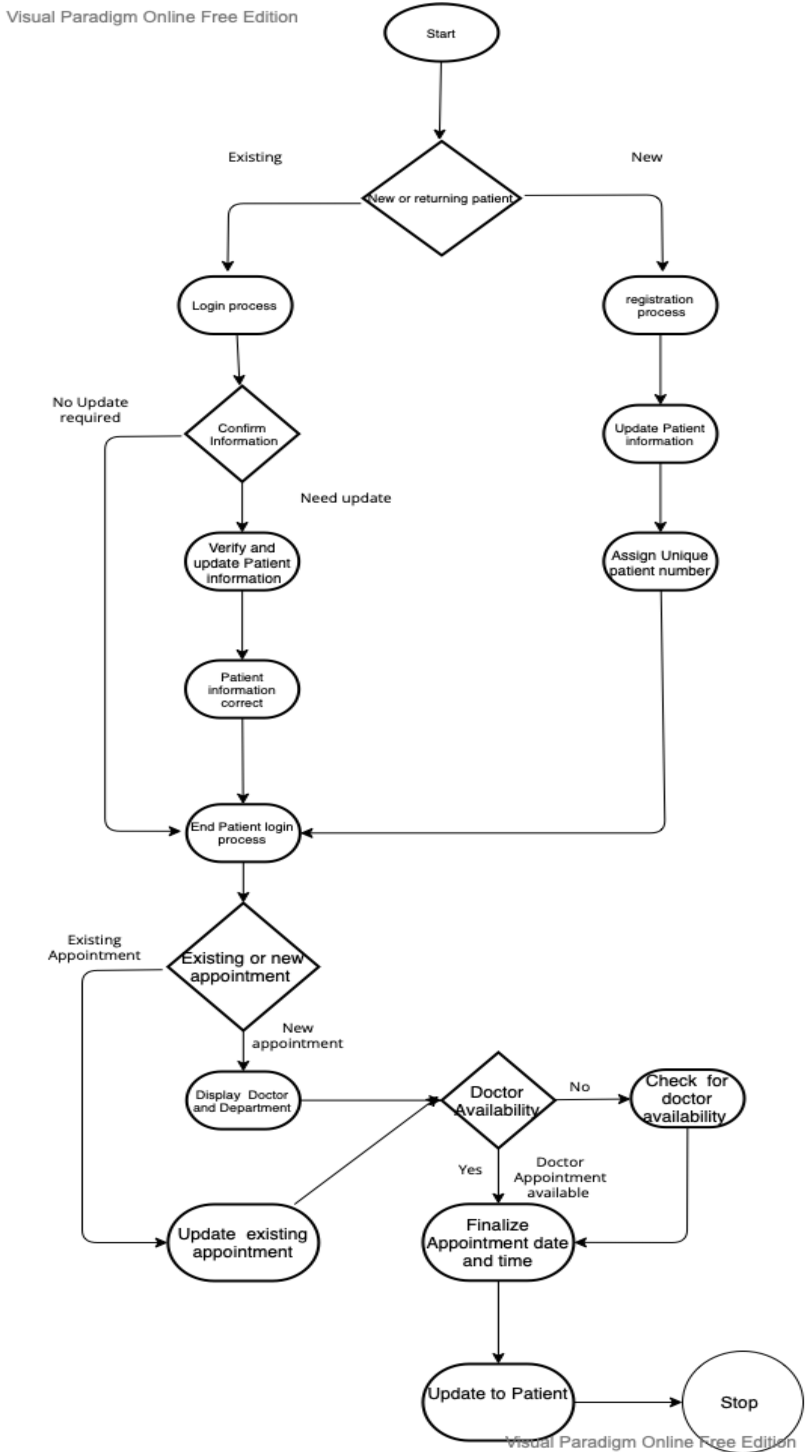

Visual Paradigm Online Free Edition
Start
Existing
New
New or returning patient
Login process
registration process
No Update required
Confirm Information
Need update
Update Patient information
Verify and update Patient information
Assign Unique patient number
Patient information correct
End Patient login process
Existing Appointment
Existing or new appointment
New appointment
Display Doctor and Department
Doctor Availability
No
Check for doctor availability
Yes
Doctor Appointment available
Update existing appointment
Finalize Appointment date and time
Update to Patient
Stop
Visual Paradigm Online Free Edition

Figure 1

5 Thread Modeling:

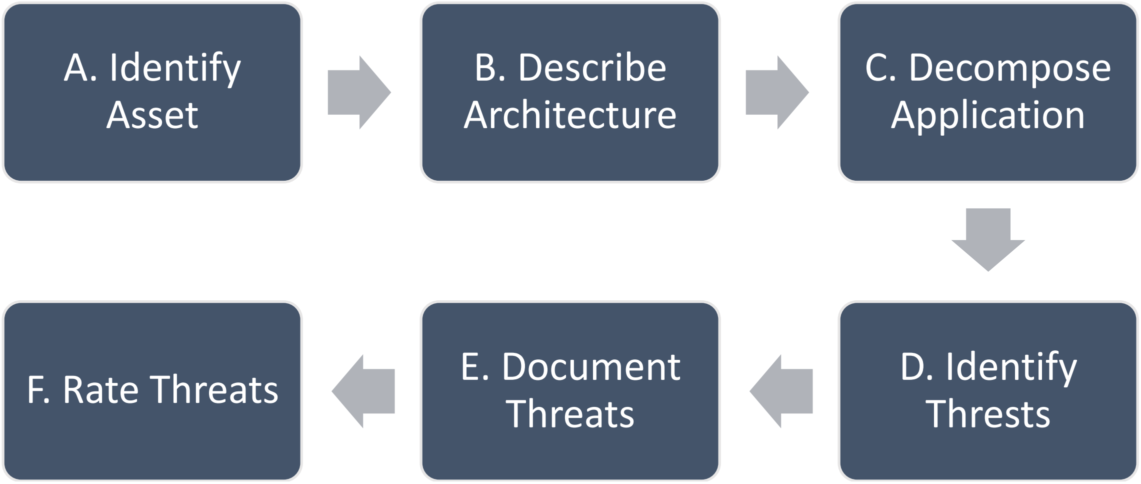
The structured approach to application tread modeling allows for the identification, quantification, and mitigation of the security risks related with the ASMIS. A possible attacker's perspective will be identified using threat modeling, as opposed to a defender's perspective. Making thread modeling a major component of the software development lifecycle (SDLC) will help in increasing application security.

By the data flow diagram identifies the system entities, events and boundaries. Successful STRIDE model can be defined using an accurate data flow diagram. STRIDE uses set of known threats, spoofing identity, tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege also defined on Table (Alhassan, et all. 2016)

Table 1

Threat	Property Violated	
Spoofing Identity	Authentication	Pretending to be something or someone other than yourself
Tampering with data	Integrity	Modifying data (Network, disk, Memory)
Repudiation	Non-repudiation	Claiming that you didn’t do something or were not responsible
Information disclosure	Confidentiality	Providing information to someone not authorized to access it
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do so

5.1 Identifying Threat modeling:



Identifying Threat Modeling Figure 2

5.1.1 Identify asset:

The following people utilise ASMIS to generate and process various types of data.

Table 2 – Identify asset

Actor	Operation / role
Doctors	- Allow doctors to view patient appointment and health information - Update health records
Patient	- Register process for new Patients - Update records for returning patients - Book appointment and review health records
Nurse	- Allow Nurse to view patient appointments - Update health records
Receptionist	- Create, Review, update and cancel patient appointment
Infrastructure and development team	- Access to database for development - Software Patch, update

Users who have been authenticated and granted permission to use the service provided by the system, as well as users who have not been authenticated or granted permission to use the service. Anyone who uses an information management system should not be alarmed by threats that arise from defects in the system's design, implementation, or setup. Identify any threats emanating from the access points in the future. Threats are defined as the objectives of an adversary, as well as their capabilities and the level of danger they represent. STRIDE is a methodology developed by Microsoft for considering threats to system security, and it serves as a reference for the classification of security concerns. (Alhassan, et all. 2016)

5.1.2 Architecture Description:

Health-related information must be stored and processed securely and confidentially, as mandated by law. Because the disclosure of a patient's medical records can have an extremely negative social impact on the patient, it is clear that appointment and scheduling management information system must have appropriate privacy safeguards in place. Healthcare professionals and IT service providers who violate privacy laws by exposing patients' confidential health information outside the ASMIS system will face severe penalties. Because of ASMIS's dangers, private health information and privacy regulations could be breached.Keeping ASMIS safe includes both information security and physical safety.

Requirements specification for the creation of Protect ASMIS is founded on the idea that it should be accessible, useable and most importantly trustworthy. As a result, the system's functionality and service are specified, and the right countermeasures to limit the ability for attackers to misuse the system are selected. As a result, threat modelling helps designers anticipate probable attack aims and formulate solutions to concerns as to what the system is implemented to defend and from whom. This is done through the use of threat modelling. Because the risks have been graded, security experts will know where to begin their research when they need to patch vulnerabilities in a present system. For large-scale projects, this is extremely critical.

5.1.3 Decompose Application

The ASMIS system flow are dhow in the Figure 3.

1. During the registration process, the patient interacts with the ASMIS User Interface (UI) and fills out the registration form. The user's information is then updated in the users database.

2. A secure method of communication will be used

3. Once the user has registered successfully, they will be given a patient ID and login information. The user will be asked for their user id and password.

4. The patient will look for an appointment in the appointment DB table, and the appointment information will be updated in the scheduling update table based on the patient's confirmation. At the same time, the appointment DB table will be updated with the doctor's availability.

5. The patient will receive confirmation.

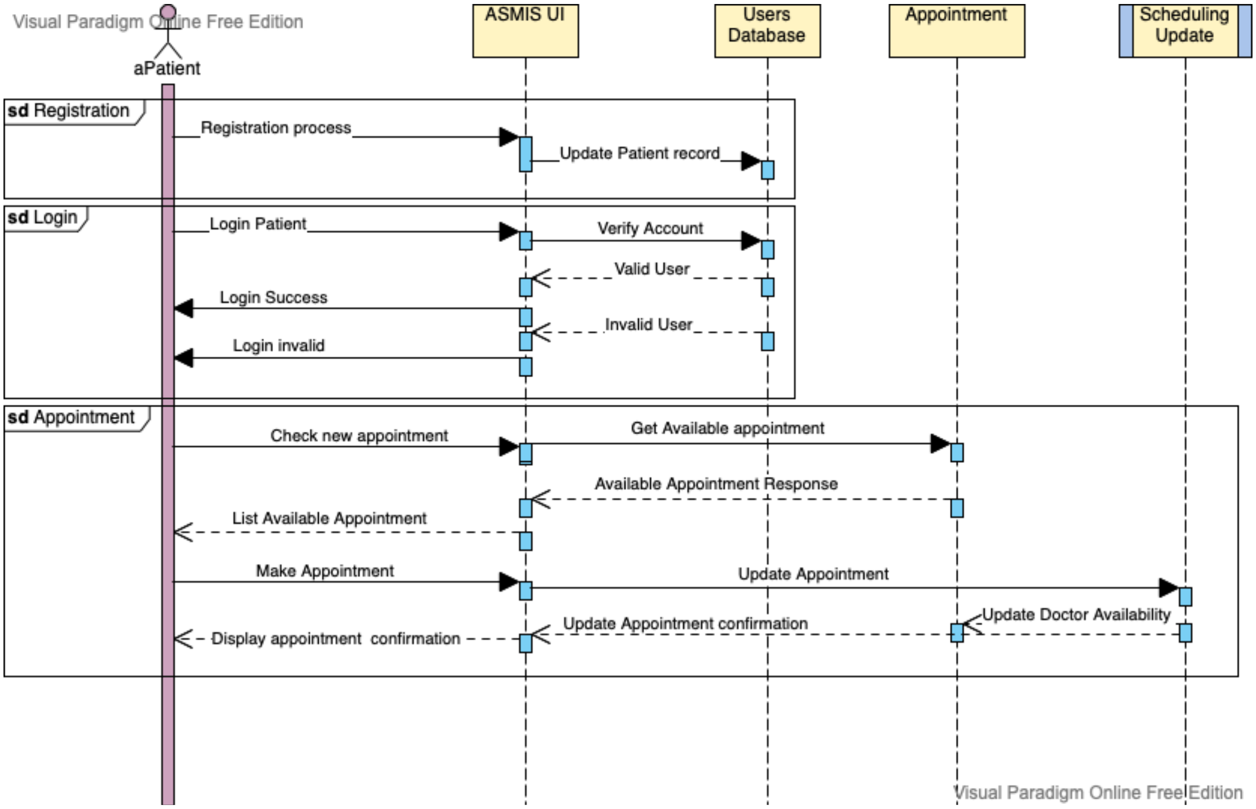


Figure 3

5.1.4 Identify Threats

The threat level can be determined by using a low, high, and medium scale. The classification of a threat as High denotes that the threat poses a high level of danger to the program and must be corrected as soon as possible by implementing the relevant countermeasures. Medium-risk threats must also be dealt with, but with less immediacy than high-risk threats. Due to the expense and time required to address a low-risk issue, it may be reasonable to overlook the threat.

With a simple rating system like the one mentioned above, it's hard for representatives of a risk analysis team or security experts to agree on the grades they give. To fix this, a methodical way of figuring out how big the real effects of a threat to security are needs to be put in place. Microsoft's DREAD model is used to figure out how risky something is. By answering the following question about a threat and using DREAD model, you can figure out how dangerous it is.

- Damage Potential: What is the potential scope of the damage if a threat is exploited?
- Reproducibility: How simple is to carry out a similar attack?
- Exploitability: What is the ease with which an attack can be launched?
- Affected Users: How many users are at risk of being affected by the assault, on a percentage basis?
- Discoverability: What is the ease with which you can discover your vulnerability?

Table 3 DREAD Threat rating scheme

	Rating	High(3)	Medium(2)	Low(1)
D	Damage Potential	Attackers get full access to system and execute and modify data	Disclose critical information	Disclose insignificant information
R	Reproducibility	Attack can be reproduced	Attack cab be reproduced, only in particular period	The attack is extremely difficult to replicate; even attackers are aware of the vulnerability.
E	Exploitability	Beginner programmer could make the attack in a short window	Trained programmer make the exploit	Attack requires and highly trained skilled person and depth knowledge

A	Affected Users	default configuration	Few users, non-standard configuration	Slight percentage of users, ambiguous feature, affected unknown users
D	Discoverability	The attack's details have been made public.	The flaw is in a part of the product that is rarely used, so only a few people should run into it.	The bug is unclear

(Openstack.org N.D)

Other infrastructure potential threats: (Shakeel, 2021)

- Analyze the potential for cyber-physical attack on application and IT facility equipment.
- Recognize possible hacker entry points into medical equipment in hospitals and healthcare facilities.
- In order to deliver a malicious outcome, a hacker or a cracker must first acquire access to a computer system, network server, or end user computers
- Protect against cyber-attacks like man-in-the-middle assaults and DOS(denial of service attacks).
- Find out if your hospital's database and web application have been hacked.

5.1.5 Document Threats

We define all potential vulnerabilities related to user identity verification and authorisation via login information that could allow unauthorised users to gain access to the system. Users' identities, login credentials, and patient medical or communication equipment are all susceptible to theft, loss, or sharing, and the most common causes are loss, sharing, and theft of these credentials. Sharing confidential user access credentials can result in a variety of problems, including misuse, alteration of sensitive patient data, and the disclosure of private information, among others. The potential harm posed by these hazards is calculated using the DREAD risk evaluation scheme.

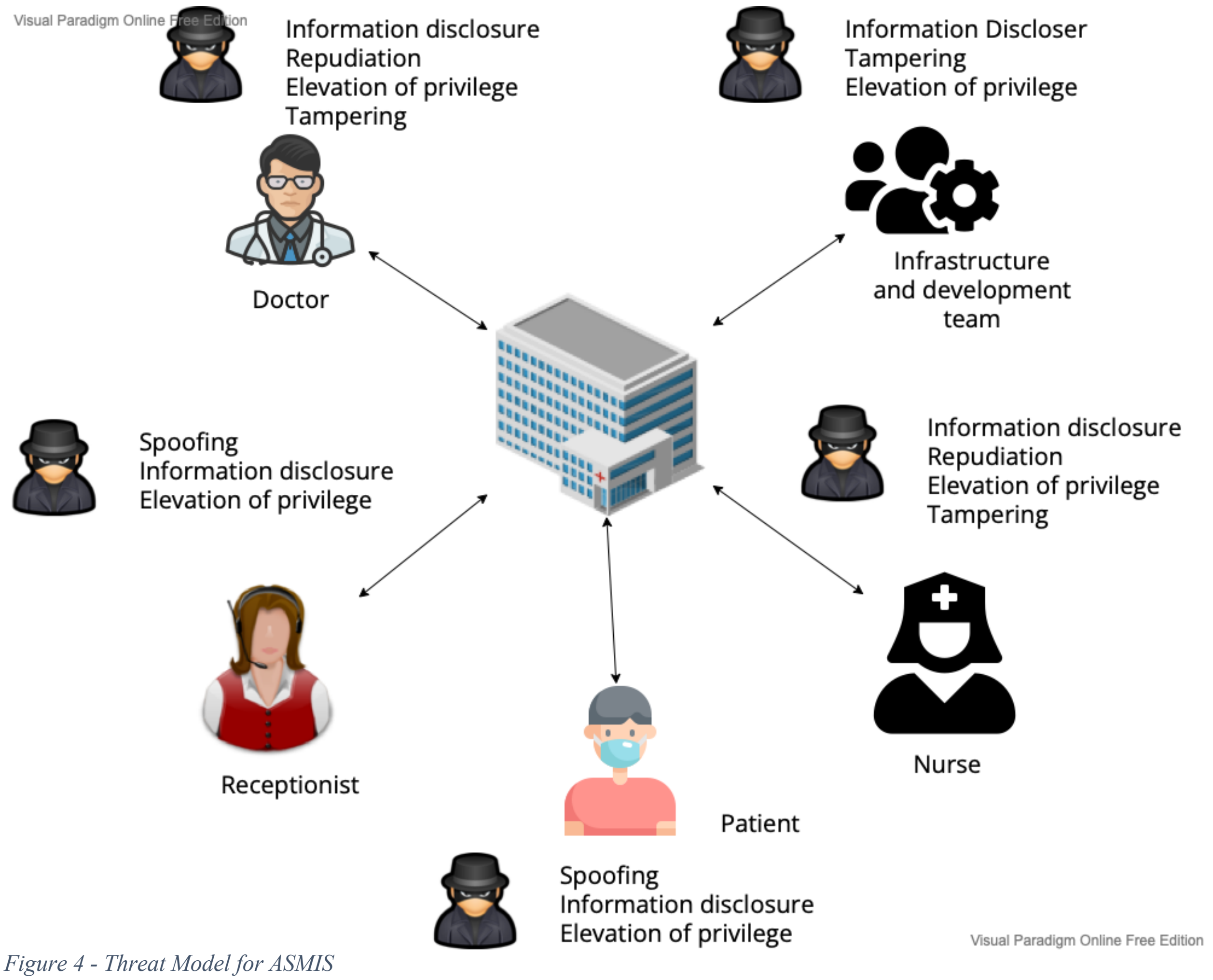


Figure 4 - Threat Model for ASMIS

5.1.6 Rate Threats

DREAD risk rating briefed in Table 3 and then put into low (0 – 6), medium (7 – 11) and high (12 – 15) groups built on how much of an effect the threat has on the ASMIS, as shown in Table 4.

Table 4 Threat rate

Threat	D	R	E	A	D	Total	Rating
Denial of service to ASMIS	3	3	2	3	2	13	High
Illegal/unauthorized access to system	3	3	3	3	3	15	High
Poor access control	2	3	2	3	2	12	High
Loss of devices with data	2	1	2	1	2	8	Medium
Personal identity spoofing	3	2	2	1	2	10	Medium
Session hijacking	2	2	1	2	2	9	Medium
Spoofing to ASMIS servers	2	2	2	1	1	8	Medium
Personal identification information spoofing	3	2	1	2	2	10	Medium
Elevation of privilege	2	3	2	2	2	11	Medium
System files tampering	2	2	2	3	2	11	Medium
Data tampering by unknow users	1	2	1	1	1	6	Low
Loss or Sharing of patient data	1	1	1	1	1	5	Low

(Openstack.org N.D)

6 Countermeasures to identified threats in the model:

The following are the countermeasure for the risk been identified using DREAD model. The designs of security systems should also be strong and redundant, able to grow, adaptable, and easy to use. And they should be able to keep going. Figure 5 shows the countermeasure against each role in the system. Erika, M, et all. (N.D)

- Separation of duty
    - Use role-based access controls and group policies to stop employees from getting to information or services that aren't needed for their jobs.
    - This can be accomplished by using software logic to ensure so each users can only access the system components that they are authorised to access and use the features that are unique to that group of users, but not tasks as well as functions that are exclusive to other user groups. (Argaw, et.al 2020)
- Least privilege
    - Make sure that employees with administrative roles have different accounts for their administrative and non-administrative work. (Miller, 2017)

- User authorization
  - Identify changes in responsibilities and avoid privileging and unauthorized access by previous workers
- Secure login with MFA
  - Use two factor authentication to secure the login
- Obscure data
  - Full data records is always not necessary, so obfuscate or mask the data wherever necessary
- Encrypted communication
  - Use secure communication between client and server and also between the servers

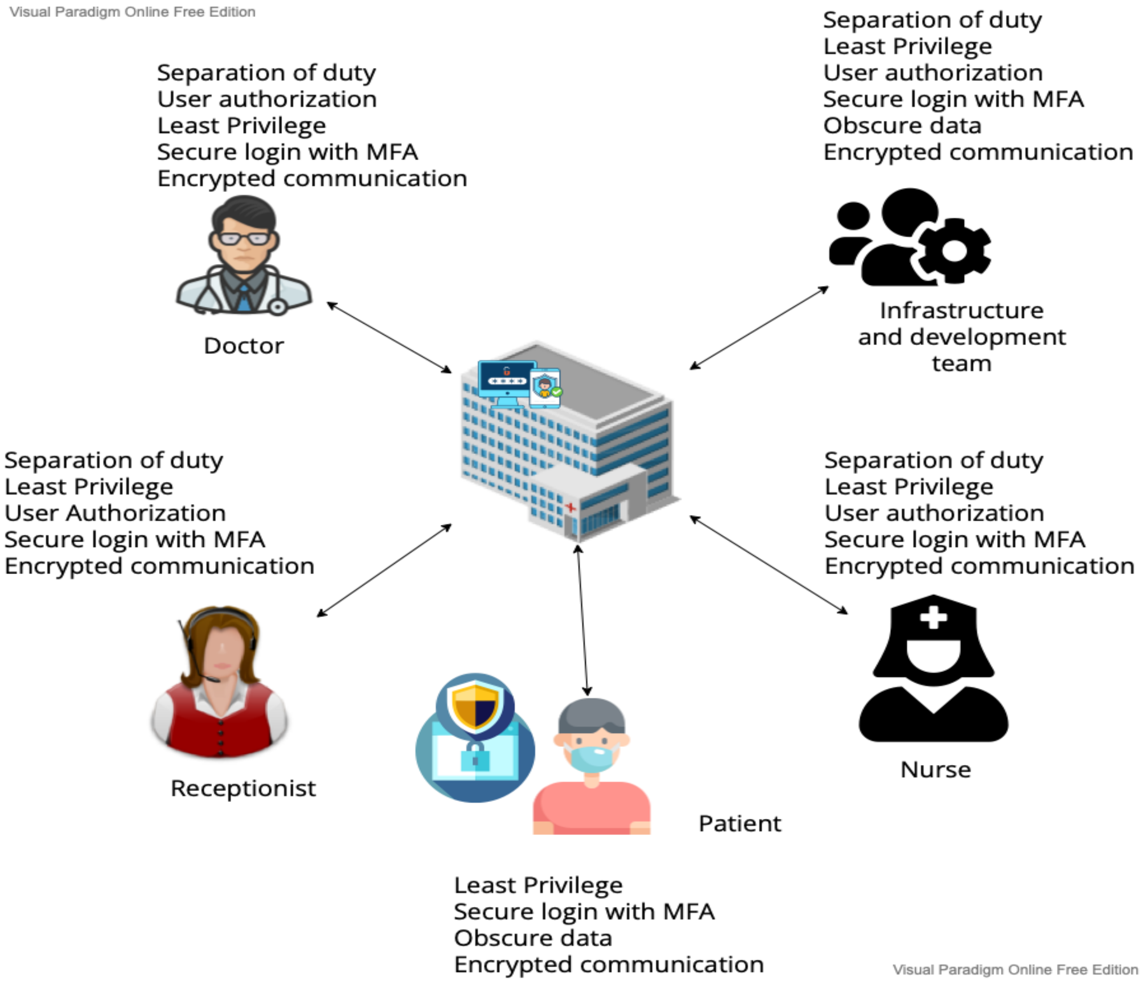


Figure 5 Countermeasure

7 Conclusion:

A threat model for an ASMIS is proposed in this document, which takes into account the various ways that an ASMIS could be attacked. For the purpose of classifying threats, a DREAD threat-risk ranking model was employed with information gathered from the STRIDE threat model. Security threats to the system's authentication and authorisation controls were examined. Due to the many risks listed in this document, security is a continuous job, and it will continue to be that way all through SDLC process.

8 Reference:

1. John K, et al. (2016) Threat Modeling of Electronic Health Systems and Mitigating Countermeasures Available from: http://ceur-ws.org/Vol-1830/Paper16.pdf [Accessed from May 2022]
2. Salem, T. et all. (2020) Available from : Cybersecurity of Hospitals https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7 [Accessed from May 2022]
3. Anon, (N.D). Available from : Security/OSSA-Metricshttps://wiki.openstack.org/wiki/Security/OSSA-Metrics
4. Infran, S. (2021) Risk management concepts and the CISSP (part 1) Available From : https://resources.infosecinstitute.com/certification/risk-management-concepts/ [Accessed from May 2022]
5. Sarah, M, (2017) Best Practices to Mitigate Insider Threats Series Available From: https://insights.sei.cmu.edu/blog/separation-of-duties-and-least-privilege-part-15-of-20-cert-best-practices-to-mitigate-insider-threats-series/ [Accessed from May 2022]
6. Erika, M, et all, Recommendation of the national institute standards and technology. Available from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf [Accessed from May 2022]