Queens Medical Centre

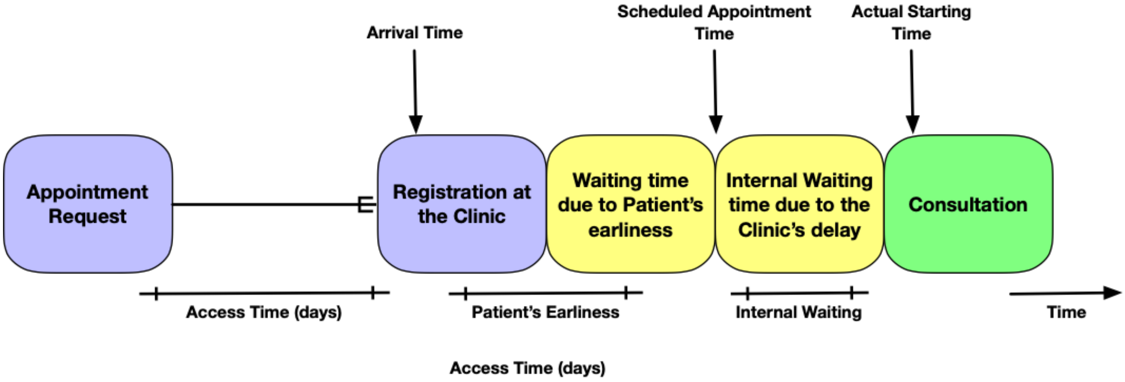
Web-based ASMIS Solution Benefits and Cybersecurity Considerations

Benefits of Web-based ASMIS System

The traditional operating model in the healthcare sector regarding registration of patients and scheduling appointments (ASMIS) both inefficient and exhausting. Under normal circumstances, patients tend to come to the Clinic and fill in the registration form and expect to be called, or patients directly call the Clinic for getting an appointment to any available time slot, including providing vital information to determine which specialist would best to attend to a given case. This in-walk or call-based patient registration and appointment scheduling processes involve several manual procedures and paperwork resulting in a bottleneck when the Clinic needs to provide the relevant healthcare services at a reasonable and constant rate. Furthermore, patient appointment scheduling and priority calls are essential to maintain the Clinic's overall service quality. However, certain areas require proper time management and quality performance. According to one of the studies, most reported issues are related to the displeasure in spending too much time before the consultation took place in clinics. In 2,710 general cases (based on the study), the average waiting time of 58 minutes per session is noted.

The depicted figure (Figure 1) below illustrates the time spend between arrival and consultation service provided by clinics. In most cases, the patient contacts the clinic administration to schedule an appointment and waits for a response until the confirmation received, which mostly takes a considerably long time or even months on some rare occasions. Once the position confirmed, patients usually required to complete a registration form upon arrival at the Clinic. The measured time between registration process and consultation in the depicted figure mostly being called as 'total waiting time', which can be broken down to the two bullets:

- Patient's earliness – Time noted between early arrival and scheduled appointment time.
- Internal waiting time – Period between the scheduled time and the actual starting time of consultation.


Arrival Time
Scheduled Appointment Time
Actual Starting Time
Appointment Request
Registration at the Clinic
Waiting time due to Patient's earliness
Internal Waiting time due to the Clinic's delay
Consultation
Access Time (days)
Patient's Earliness
Internal Waiting
Time
Access Time (days)

The current business processes and procedures in the Clinic depends on the first-in, first-out (FIFO) principle where leads to several consultation services:

In the walk-in appointments, patients should be completing forms before handing over identity document to the clinic administration personnel to ease the complex registration process. However, this process needs to be repeated for each of the visits; thus, it results in inefficient hardcopy forms and a less effective management method.

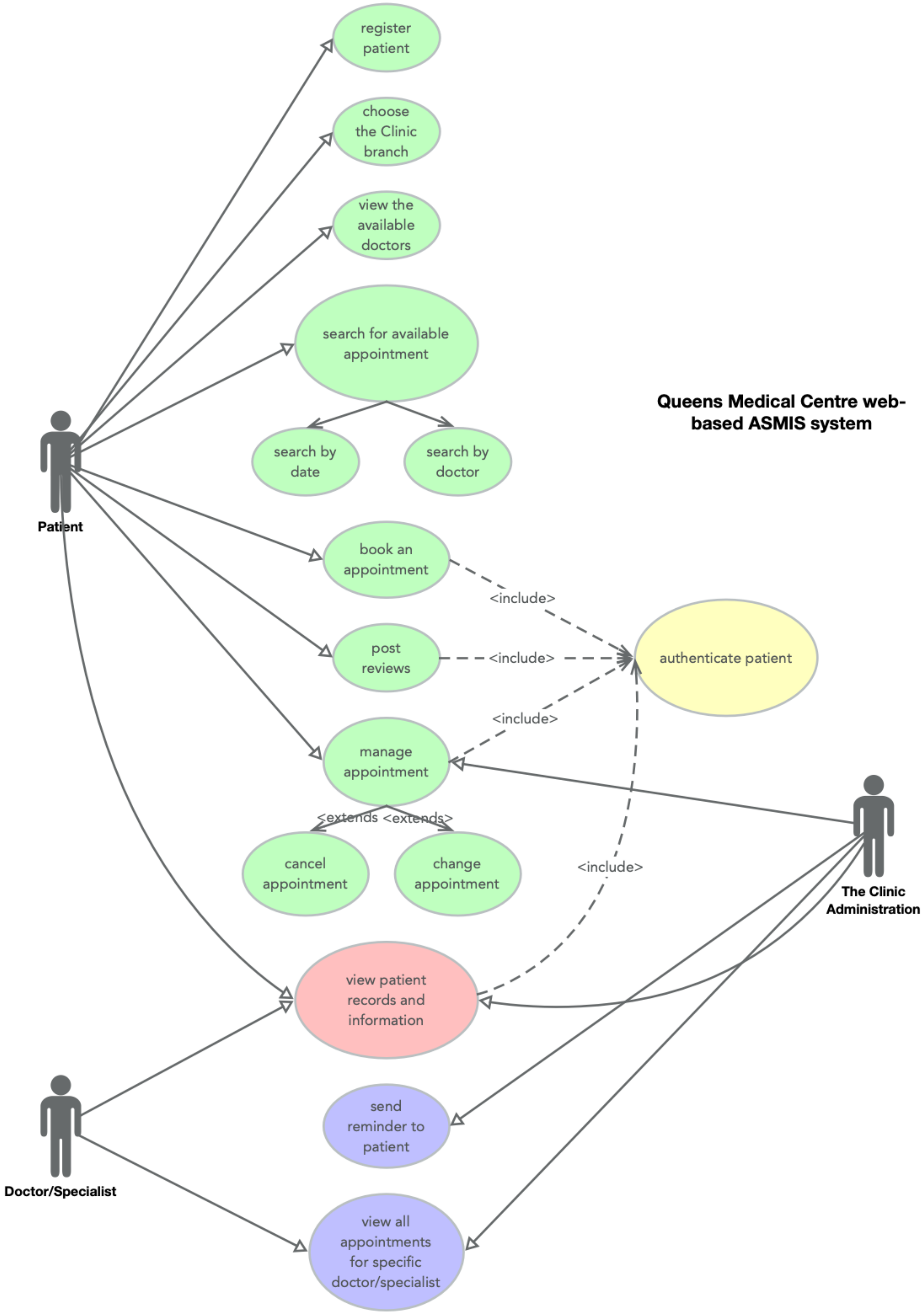
One of the other ways of getting a professional healthcare service is scheduling an appointment to call the Clinic before the visit. However, available time slots manually need to be confirmed by the clinic administration personnel, including not easy to predict waiting time period for patients.

For the last two decades, there have been many technological advancements, including in the healthcare industry. Nowadays most organisations depend on IT systems to deliver reliable services. To overcome the challenges mentioned earlier and enhance the traditional operating model, Queens Medical Centre could leverage advancements in the technology space by using web-based ASMIS solutions. It could contribute to the refinement of the conventional operational model, including evading the annoyance of lining up and filling forms. In addition to that, there might be other advantages for the clinic personnel such as monitoring patient's status, automatically sending notifications to the clinic staff and patients on upcoming appointments, effortlessly searching for any sensitive data or personal information since it could available online.

Furthermore, a web-based ASMIS system also allows a patient to complete forms and book appointments in accordance with their time suitability without waiting in the line, including making it possible to store the relevant records and data in the electronic environment. However, there might be potential cyber threats as well concerning the use of these systems. These potential cyber threats could be depended on the proposed technical setup, deployment model (e.g., a cloud-based or local deployment), and the data (e.g., credit card data for payments, identification number, social security number, past medical records, etc.) stored in the system. For instance, public internet-facing interfaces could be overtaken because of known and not timely fixed vulnerabilities, both personal and sensitive data stored in the system could be easily compromised due to not encrypting data at rest or inflow, etc.

UML Use Case Diagram of the Web-based ASMIS System

One of the main objective of use case diagrams is to illustrate use cases in the system. There could be several elements in the use case diagrams, such as actors, use cases, and relationships. These diagrams also mainly being used to show aspects and use cases of the system in question. Additionally, these diagrams focus on functionalities of the system and provide insights regarding the relevant requirements, including describing "what". The depicted figure (Figure 2) below illustrates what a web-based ASMIS system looks like, including different aspects of the system.

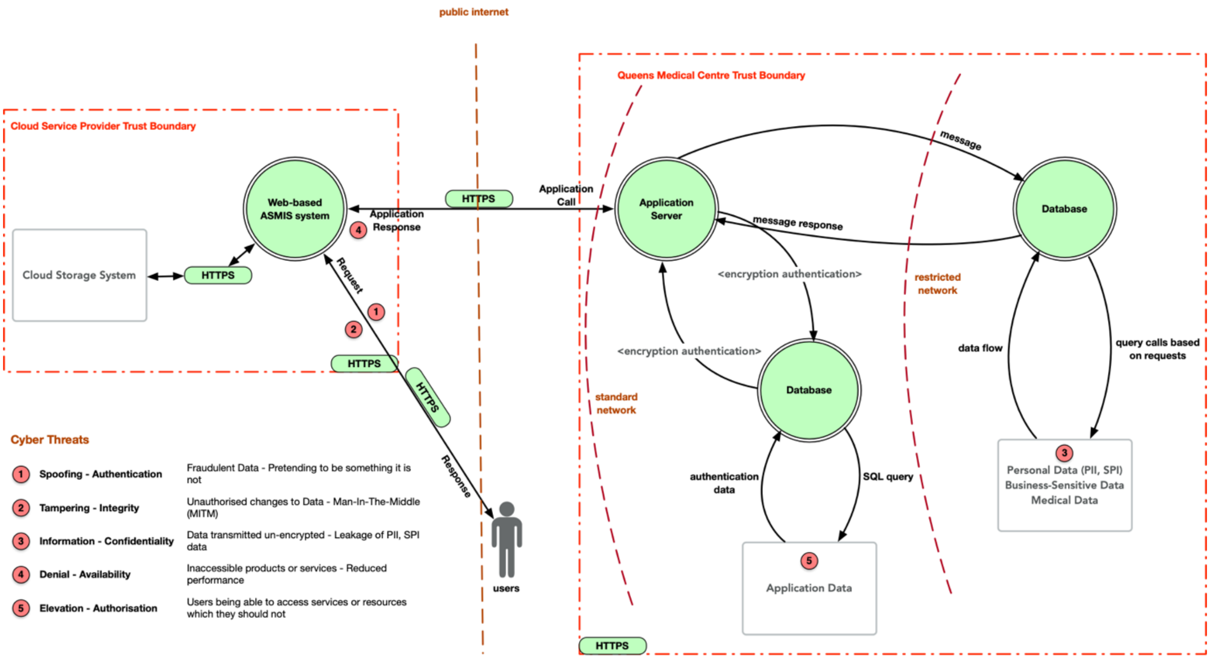

register patient
choose the Clinic branch
view the available doctors
search for available appointment
search by date
search by doctor
Queens Medical Centre web-based ASMIS system
Patient
book an appointment
<include>
post reviews
<include>
authenticate patient
<include>
manage appointment
<extends
<extends>
cancel appointment
change appointment
<include>
The Clinic Administration
view patient records and information
send reminder to patient
Doctor/Specialist
view all appointments for specific doctor/specialist

UML Threat Modelling Diagram of the Web-based ASMIS System

A threat model is a different form of risk management where the technical teams try to identify possible threats and vulnerabilities. For example, in many mid to large organisations, development and operation teams conduct a session with the participation of cybersecurity experts to list out all potential threats, analyse their impacts and magnitudes, and formulate a solution when presenting the detailed threat model.

There are many threat modelling approaches developed recently to answer increasingly sophisticated cyber threats. However, before considering any security-related considerations or controls, an appropriate threat modelling technique should be considered. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) is one of the widely recognised threat models in cyberspace. STRIDE includes several threat groups where could be used for proper classification of threats by operational and technical teams before implementing or deploying the relevant system.

The depicted figure (Figure 3) below describes the possible threats relevant to the Queens Medical Centre Web-based ASMIS system:


public internet
Cloud Service Provider Trust Boundary
Web-based ASMIS system
Cloud Storage System
HTTPS
HTTPS
Application Call
Application Response
4
Request
1
2
HTTPS
HTTPS
Response
users
Queens Medical Centre Trust Boundary
Application Server
message
message response
Database
<encryption authentication>
<encryption authentication>
restricted network
standard network
Database
data flow
query calls based on requests
3
Personal Data (PII, SPI)
Business-Sensitive Data
Medical Data
authentication data
SQL query
5
Application Data
HTTPS
Cyber Threats
1 Spoofing - Authentication
Fraudulent Data - Pretending to be something it is not
2 Tampering - Integrity
Unauthorised changes to Data - Man-In-The-Middle (MITM)
3 Information - Confidentiality
Data transmitted un-encrypted - Leakage of PII, SPI data
4 Denial - Availability
Inaccessible products or services - Reduced performance
5 Elevation - Authorisation
Users being able to access services or resources which they should not

Cybersecurity Considerations

Several pre-requisites should be completed before concluding cybersecurity considerations, such as possible mitigation actions or safeguards to minimise the impact of the relevant adversaries. For instance, performing a business impact analysis (BIA) could help to determine the criticality of the Web-based ASMIS system's criticality. Or the STRIDE-based threat model (including Figure 2 and Figure 3) and the use case diagram could be used in conjunction for preparing precise analyses and specifications of security requirements. For example, although a Web-based ASMIS system improves the quality of the provided services for the Clinic, digitalising medical records, collecting and storing patient's data, provisioning patient data and transmitting it throughout public networks arise new data security risks for the Clinic. If technical and operational teams mentioned earlier do not consider these possible threats, then the Clinic could not operate in an acceptable manner, including not adequately safeguarded Web-based ASMIS system vulnerable to incidents or security breaches.

As the next logical step of the threat modelling, focusing on its components come next. These components could be, identifying assets, determining the trust level of systems and users, listing the relevant threat agents, identifying and classifying threats based on the STRIDE. Once we complete these additional steps, security measures could be determined for each of the relevant threats for the Clinic.

Identification of Assets: An asset could be anything valuable for an organisation that needs to be adequately protected from adversaries. Threat models or business impact analyses could be used to measure how valuable or critical the asset. The following table (Table 1) describes the identified assets based on the threat model.

ID	Asset	Description
Assets relating to Web-based ASMIS system, database and application data		
A1.1	Patient credentials	The login credentials used by a user to log into the Web-based ASMIS system
A1.2	Patient communication equipment	Typical equipment (e.g., mobile phone, tablet, PC, etc.) used by users to display, collect, store or transmit particular data
A1.2.1	Communication equipment credentials	Equipment-related data, such as an equipment identifier and key
A1.2.2	Web-based ASMIS system	
A1.2.3	Patient-related data	The patient communication equipment will store data associated with a patient. This data could include the patient’s name, forename, identifier, etc.

Assets related to the Clinic’s core infrastructure		
A2.1	Personal/Medical/Financial records database	All patient-related data (A1.2.3) transmitted and stored in the database located in the restricted network. Data from medical equipment (A1.2) stored as well
A3.1	User credentials	Login credentials used by the Clinic personnel (e.g., doctors, specialists, administration staff, etc.)
A3.2	Application Server	Provides underlying infrastructure-level services and orchestrate communication and data flows between the web-based system and databases.
A3.3	Patient-related data	Information related to the patients (A1.2.3) retrieved by specialists/doctors. Any patient-related data can be altered or added by the Clinic’s staff (e.g., appointment schedules and past examinations, follow-up plans, etc.)

**STRIDE-base threat modelling work significantly originated from the paper called 'A stride-based threat model for telehealth systems’ which referenced in the references.*

Trust Levels of Users and Threat Agents: Trust levels indicate authorisation for entities such as users, equipment and systems. The following table (Table 2) describes the relevant threat agents.

ID	Threat Agent	Description
Patient		
TA1.1	Patient with valid login credentials	A patient who uses A1.2.2 with valid login credentials
TA1.2	Patient with invalid login credentials	A user (forcing someone who authorised) who uses A1.2.2 and is attempting to log in with invalid login credentials
The Clinic Personnel		
TA2.1	The Clinic personnel with valid login credentials	A user (e.g., doctor, personnel, etc.) who is connected to A3.2 with valid login credentials
TA2.2	User with invalid login credentials	A user (forcing the clinic personnel) who is connected to A3.2 and is attempting to log in with invalid login credentials
Administrator		
TA3.1	Application Server & Database Administrator	The database server administrator who has administrative privileges to the database (A2.1) used for storing personal/medical data
TA3.2	Web-based ASMIS Administrator	The Web-based ASMIS Administrator can configure the system for A3.2
Other Components		
TA4.1	Patient communication equipment	Equipment that provides a user interface for the patients to support collection, the transmission of data and information from the Clinic
TA4.2	Personal/Medical/Financial records database	Database servers used to store patient-related data (A1.2.3)

Identification and Classification of Threats – STRIDE: The following table (Table 3) below describes the classified threats that grouped based on the their types: authentication, authorisation and access and data security.

Authentication Threats				
ID	**Threat Description**	**Threat Agent**	**STRIDE**	**Impact**
T1.1	Patient identity loss or identity sharing	TA1.1	S	Low
T1.2	Personnel identity loss or identity sharing	TA2.1, TA3.1, TA3.2	S	High
T1.3	Identity theft and misuse (the Clinic system administrators)	TA3.1, TA3.2	S	High
T1.4	Spoofing of source – servers and databases used to store personal data and medical records may be spoofed by attackers	TA4.2	S	High
Authorisation and Access Threats				
ID	**Threat Description**	**Threat Agent**	**STRIDE**	**Impact**
T2.1	Unauthorised access to the data using shared or stolen passwords	TA1.1, TA2.1	E	High
T2.2	The Clinic system administrators get intentional unauthorised access to patient data for malicious intents	TA2.1, TA3.2, A3.3	E	High
T2.3	Data tampering: The Clinic personnel (doctor, specialist) and system administrators intentionally or unintentionally add/delete/modify data due to excessive privileges	TA2.1, TA3.2, A3.3	T	High
T2.4	Unauthorised access to management interfaces	TA1.1, TA 2.1, TA3.2, A3.3	E	High

Data Security Threats				
ID	**Threat Description**	**Threat Agent**	**STRIDE**	**Impact**
T3.1	Unauthorised disclosure: patients unintentionally access some confidential data due to compromised (e.g., malware) communication equipment	TA1.1	I	Low
T3.2	Unauthorised disclosure: The Clinic personnel (doctor, specialist) and system administrators intentionally or unintentionally access some confidential data due to compromised (e.g., malware) workstations	TA2.1, TA3.1, TA3.2, A3.3	I	High

Identified Threats and Security Measures – STRIDE: The main objective of developing a threat model for the Clinic's Web-based ASMIS system is to properly harden and enhance the system's cybersecurity to protect both the Clinic's and patients' valuable assets from potential security threats. The following table (Table 4) below describes the identified threats and security measures.

STRIDE	Threats	Security Measures
Spoofing	T1.1, T1.2, T1.3, T1.4	- Robust authentication: Patients and users must be authenticated to the system using a firm password policy and multi-factor authentication mechanisms - Encryption: All credentials must be encrypted and ensured to not transmitted in clear text form

		- Cryptography: Cryptographic protocols such as TLS must be used for secure communication between system components
Tampering	T2.3	- Firm Authorisation: Role-based access control (RBAC) must be deployed with the least privileges and separation of duties principles. Patients and users must be assigned to access with a need-to-know basis - Data hashing and signing: All confidential data must be hashed and signed to ensure that the data is valid (e.g., untampered and authentic) - Secure Intercommunication: The communication links between system components must be ensured by using protocols that provide message integrity and confidentiality
Information Disclosure	T3.1, T3.2	- Strong authorisation: Robust access control mechanisms deployed, and only authorised users could access to data - Encryption: Ensure that all sensitive data (e.g., personal data, medical records, etc.) is encrypted and only authorised users could access or read this data - Secure Intercommunication: The communication links between system components must be ensured by using protocols that provide message integrity and confidentiality
Elevation of Privilege	T1.3, T2.1, T2.2, T2.3, T2.4	- Principle of least privilege: All authorised users must have a need-to-know basis minimum required access

References:

Abomhara, M., Gerdes, M. and Køien, G.M. (2015) 'A stride-based threat model for telehealth systems', *NISK Journal*. pp.82-96. Vancouver

Alhassan, J.K., Abba, E., Olaniyi, O.M. and Waziri, V.O. (2016) 'Threat modeling of electronic health systems and mitigating countermeasures' In *International Conference on Information and Communication Technology and Its Applications (ICTA 2016).* Federal University of Technology*,* Minna*,* November*.* Nigeria.

Symey, Y., Sankaranarayanan, S. and binti Sait, S.N., 2013. Application of smart technologies for mobile patient appointment system. *International Journal*, *2*(4), p.7.

Siau, K. and Lee, L., 2004. Are use case and class diagrams complementary in requirements analysis? An experimental study on use case and class diagrams in UML. *Requirements engineering*, *9*(4), pp.229-237.

Johnstone, M.N., 2010. Threat modelling with STRIDE and UML.

Hasan, R., Myagmar, S., Lee, A.J. and Yurcik, W., 2005, November. Toward a threat model for storage systems. In *Proceedings of the 2005 ACM workshop on Storage security and survivability* (pp. 94-102).

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B.J. and Simoes, E., 2017. Web-based medical appointment systems: A systematic review. *Journal of medical Internet research*, *19*(4), p.e134.