Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 3, Issue 5, 2025

A STRIDE BASED APPROACH TO FORTIFY DIGITAL HEALTHCARE SECURITY

Summia Aziz[*1], **Dr. Shariq Hussain**[2]

[*1]*MS (Computer Science)*
[2]*Department of Software Engineering, Foundation University Islamabad*

DOI: https://doi.org/10.5281/zenodo.15381629

Keywords

Article History
Received on 03 April 2025
Accepted on 03 May 2025
Published on 10 May 2025

Copyright @Author
Corresponding Author: *
Summia Aziz

Abstract

The study underscores the paramount significance of robust threat identification in Smart Health Systems (SHS) to enhance reliability and practicality. This study employs a methodology that effectively utilizes the Microsoft Threat Modelling Tool, leveraging the STRIDE framework, to comprehensively identify threats within the SHS. Through the incorporation of the DREAD model, this approach facilitates efficient risk management, prioritizing threats based on Damage, Reproducibility, Exploitability, Affected Users, and Discoverability. The systematic framework proposed in this research proves instrumental in identifying threats at early stages, streamlining the mitigation process, and contributing to the overall security resilience of Smart Health Systems. This work aims to fortify the foundation of SHS by addressing security challenges proactively, ensuring a reliable and secure digital healthcare ecosystem.

INTRODUCTION

A new era in the healthcare system has begun due to digital transformation. Smart healthcare systems are garnering the attention of experts because they can significantly enhance healthcare services and streamline medical processes. Through the use of technologies like IoT, artificial intelligence, and cloud computing, these systems not only collect medical data but also analyse and manage it. The development of the latest Smart Healthcare Systems relies on a suite of advanced technologies(Abaoud, Almuqrin, and Khan 2023).

Internet of Things (IoT) devices, like sensors and wearables, play a pivotal role by continuously collecting real-time health data. This data is then securely transmitted to the cloud for storage and analysis, aided by cloud computing technology. Artificial Intelligence (AI) algorithms are applied to interpret and extract meaningful insights from the data, helping in medical decision-making. The use of blockchain technology ensures the integrity and privacy of patient health records (Minopoulos et al. 2022).

These systems prioritize data security and privacy through encryption, access controls, and patient-consent mechanisms, granting authorized healthcare professionals access to patient data. In the real world, these technologies have brought about a healthcare revolution, enabling remote monitoring, early disease detection, and personalized car (Rahaman et al. 2023).

(Perez-Pozuelo et al. 2020) Addressed that wearable devices empower individuals to take control of their health, while data-driven insights lead to improved treatment outcomes. In summary, Smart Healthcare Systems are making healthcare more efficient, accessible, and personalized, thereby contributing to a healthier world, supported by robust data security and patient privacy measures. No doubt these advanced healthcare systems are making healthcare more accessible for patients and healthcare professionals but due to the heavy reliance on technology, there are also numerous critical security concerns related to sensitive patient data (Ali et al. 2022).It is evident that in real word application of smart health care system, data security and patient privacy are critical challenges because a vast amount of data is seamlessly shared via sensors and then stored in medical records or presented in clinics. The insiders often have the necessary credentials to carry out data breaches or other cyber risks. In some cases, disgruntled employees may steal Protected Health Information (PHI) and expose it online as an act of revenge against their employers. This threat may involve individual actions or collusion with employees from other organizations or criminal groups. While connected technologies bring numerous benefits, they also become attractive targets for cyberattacks and data breaches (Kumari et al. 2023).Although external breaches tend to dominate discussions of security risks, internal misuse is more prevalent in the healthcare industry than in many other sectors. (Rani et al. 2023) describes that Internet of Medical Things (IoMT) devices are designed to enhance patient care, are also enticing targets for cybercriminals seeking valuable health information. To ensure the safety of patients and their data, it's imperative for manufacturers to integrate security measures right from the design stage.

Protecting sensitive healthcare data is paramount in the face of growing cyber threats. Healthcare's reliance on technology introduces unique security and privacy challenges. Insiders, whether willingly or under duress, can pose significant threats to patient data. Implementing cost-effective security measures like multi-factor authentication is crucial (Almagrabi 2023) .The digitization of healthcare has increased the complexity of safeguarding Protected Health Information. Mobile logins and medical device security can create vulnerabilities (Mahmoud et al. 2023).Medical equipment websites are appealing targets for hackers, and as the Internet of Medical Things (IoMT) grows, data interception becomes a concern. Data breaches are common due to human error, necessitating robust information security management. Healthcare institutions must prioritise cybersecurity to protect patient records from ransomware attacks and phishing threats. STRIDE, initially introduced by Microsoft, serves as a mnemonic for identifying potential threats within a system. It encompasses Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. The method involves modelling threats using a data flow diagram to represent the system in question. In the STRIDE analysis, the system components are evaluated against six primary security properties: confidentiality, integrity, availability, authentication, authorisation, and non-repudiation. Although very effective, the literature reports a lack of strategy for applying STRIDE on Cyber-Physical Systems (CPS). This procedure allows for the systematic analysis on a landscape of threats to determine gaps in the mechanism thus providing full plethora prospects having a likelihood of attacks. Data flow diagrams allow for more detailed research of security properties, making it possible to get a better idea about the system construction and interactions.

1.1.1 Cybersecurity and Smart Healthcare Systems

Below are various regulations and standards addressing cybersecurity in the healthcare sector. Health Insurance Portability and Accountability Act (HIPAA): The United States Department of Health and Human Services (HHS) is a federal law that safeguards the protection and confidentiality of healthcare data. The HIPAA Security Rule in particular, sets the standards of how to safeguard electronic protected health information (ePHI).

Health Information Trust Alliance (HITRUST): The HITRUST framework combines multiple standards (such as HIPAA, NIST and ISO) to help organizations manage cybersecurity and risk. The healthcare sector widely use HITRUST Common Security Framework (CSF).

National Institute of Standards and Technology (NIST) Cybersecurity Framework: The NIST Cybersecurity Framework is a robust solution that many organizations, in healthcare and more widely across sectors adopt as it helps manage cybersecurity risk. The NIST framework is a linchpin for many healthcare organizations' cybersecurity efforts.

Centres for Medicare & Medicaid Services (CMS) Rules: There are regulations within the Centers for Medicare & Medicaid Services (CMS) that govern the methods by which patient data must be secured with respect to healthcare providers who participate in Medicare and Medicaid programs. This means that these regulations tend to line up with good cybersecurity practices.

European General Data Protection Regulation (GDPR): Healthcare providers that participate in Medicare and Medicaid programs are subject to specific patient data security regulations from the Centers for Medicare & Medicaid Services (CMS) these laws generally comply with general cybersecurity protocols.

Medical Device Cybersecurity: For example, the U.S. Food and Drug Administration (FDA) has a set of rules that you should follow to secure a medical device. It is advised that manufacturers and healthcare providers comply with these dictates to guarantee their products are safe and secure and pose no risk to patient safety. Rapid change in cybersecurity cause a huge change in regulations, principals and protocols. To cope with these emerging changes organizations should periodically update these protocols, laws and rules. This practice will help organizations to stay updated and identify threats easily.

1.2 Background/Knowledge Gap

Healthcare organizations are not only interested in collecting patients' data but also want to make it digitalized. They want it to be a personalized service so patients can get benefits. However, the digital progress carries with it essential issues concerning data protection and patient confidentiality. Electronic health records, diagnostic reports and monitoring data cannot be more sensitive. The data breaches can result in identity theft, financial fraud and patient care compromised.

Existing literature, as mentioned by Rahaman et al. Smart Healthcare Systems (2023), there is frequently a lack of full-fledged frameworks specifically developed for the obstacles faced by them. Existing solutions tend to target a specific security aspect, uniquely focusing on problems like encryption or access control but not doing so systematically towards issuance of healthcare institutions and practitioner candidates themselves. (Albahri et al. 2023) the authors discussed necessity of adaptable and scalable security measures that can keep up with all dynamical developments in healthcare systems. With the pace of evolution of healthcare technologies and threats, more thorough investigation should be done for the ability to incorporate tomorrow's risks into security frameworks

Although we talk much about the technical aspects of data security, the patient-centric view to privacy is frequently missing. The integration of patients' concerns, rights, and preferences into security frameworks is essential in empowering individuals with the ability to govern their personal health information. There are a lot of literature suggesting solutions from theoretical perspective but there is not enough study over practical challenges of data security and its real world implementations in healthcare sector. Filling this gap is integral in converting our theoretical frameworks to actionable practices.

The healthcare space is subject to many standards, such as HIPAA and GDPR. This is a huge knowledge gap as trying to keep up with regulatory compliance, while keeping the networks both secure and private seems like an almost impossible task.

Addressing these gaps is crucial for developing an effective framework that ensures data security and patient privacy in Smart Healthcare Systems. Patients should have control over their health data (Xu et al. 2023).However, the challenge lies in designing systems and policies that respect patient privacy preferences while still allowing for the secure sharing of data for medical purposes. It should ensure a secure doctor patient relationship. The inherent sensitivity of this data makes it an attractive target for cyberattacks and unauthorized access, putting patients' personal information at risk i.e. patient data is being monetized without patients' informed consent and data tampering etc (Almagrabi 2023).

Cybersecurity Threats: The healthcare sector has become a primary target for cybercriminals, leading to a surge in data breaches, ransomware attacks, and medical record theft. The ever-evolving nature of cybersecurity threats poses an ongoing challenge to safeguarding patient data (Thomas and Ngalamou 2022).

Inadequate Security Measures: Many healthcare systems may lack sufficient security measures to protect against evolving threats. Outdated or insufficient security protocols leave vulnerabilities open for exploitation. Similarly, the rapid adoption of emerging technologies in healthcare, such as IoT and cloud computing, introduces novel security and privacy challenges that are not yet fully understood.

Smart Healthcare system provides data exchange between different entities in the Smart Eco-System — like healthcare providers, insurers, researchers and patients. This increasing myriad of systems adds to the complexity of data governance, data security and privacy requirements that must be met. The challenge is the same for ensuring access to authorized personnel, like healthcare professionals and preventing access by unauthorized. Granular access control with frictionless data migration continues to be a challenge.

To address some of these issues, various threat models must be formed for accurately identifying and characterizing threats in this section, we evaluate three well-known threat models. CIA The STRIDE model details six threat types, that together violate different security properties:

Spoofing: Performs identity fraud by circumventing authentication. Like a doctor or admin account logging in without permission to harvest confidential patient data.

Tampering: Comprises illicit data tampering, breach of integrity. When medical documents are tampered with it can put patient's life at risk due to incorrect records.

Repudiation: This is the act of caring out some malicious action which can be not traced to you (broken non-repudiation). It helps hide an attacker's actions to make detection and cleanup more difficult.

Information Disclosure: Results in breach of confidentiality and release of confidential information. Such activities can involve accessing confidential patient data without authorization.

Denial of Service: Entails the information being made unavailable to legitimate users and thus violates availability. This in turn has a potential to delay care, and thereby affect the risk of life for the patient.

Elevation of Privilege: Defining (or) gaining more user rights than provided against the User ACT-Authorization GrossXXX (Input Stream Input Stream, Output Stream Output Stream), This could make attacks more serious.

Confidentiality: The InfoSec foundation CIA model, with it comes three essential security properties.

Integrity: Seeks to secure confidential data from other parties. Patient information will need to be guarded with encryption, strong authentication and training against phishing.

Availability: To prevent the falsification of information that could lead to potentially life threatening outcomes for patients. This threat is mitigated using measures like storage encryption and encrypted communication protocols.

Focuses on the never-ending access to data to only those who are authorized. Lack of availability, from attacks to misconfigurations but also hardware failures or simple acts of God such as natural disasters can mean patient lives on the line. In mitigation strategies: using redundant hardware, effective backup strategy, cloud computing and monitoring tools.

These models offer a complete top-level view of the various dynamics in the vast healthcare cybersecurity ecosphere, allowing us to appreciate threats and challenges concerning those subjects. Having identified such concerns, the identification of these issues will be significant in designing a robust framework that can guarantee data security and patient privacy in Smart Healthcare Systems. Addressing these challenges is crucial to ensuring patient data are secure, and that the opportunity presented by emerging healthcare technologies is realized.

1.3 Problem Statement

Cybersecurity and data privacy lead to a predominant challenge in the healthcare sector such as unauthorized access, and cyberattacks. In other words, a violation of doctor-patient secrecy (including sensitive healthcare information). Partly in reaction to these challenges, there is a long-standing imperative to create such an all-encompassing security framework able to answer this particular set of threats.

1.4 Objective of Study

The following are the aims of this proposed research

- Identify and categorize security and data privacy threats within healthcare systems with the STRIDE framework.
- Evaluate existing security measures and policies, and assess their effectiveness in mitigating STRIDE-related threats.

1.5 Significance of the Study

The work focuses on the current top issues of security and privacy in patient data to build a reliable smart healthcare system. Healthcare, like every other industry in the challenging digital world today, is adopting technologies such as IoT (Internet of Things), AI (Artificial Intelligence) and data analytics to improve healthcare services and patient experience. Unfortunately, these improvements introduce significant security and privacy concerns that need to be addressed. This study aims to provide robust security for patient data. When patients put their trust in a healthcare system, the most sensitive details of medical information are shared with these systems and any breach cannot only prove to be dangerous for patient safety but also detrimental to his/her own well-being. This study will contribute to the enhancement of strong security mechanisms and privacy protections thereby protecting patient data from access overreach and hence support the important facet of trust between patients, and health consumers including indigenous communities (towards health system). Additionally, the research has implications on legal and ethical grounds. The response to this question has applications not just for patient care, but also information corresponding with regulations such as the General Data Protection Regulation (GDPR) which is very important related to healthcare. Noncompliance can create legal consequences and damper an institution's reputation. In this regard, the present study sought to support health systems in following national and international guidelines that consider these regulations, thereby allowing legal risk reduction as well as respect for ethical principles. In considering these critical matters, the study adds to improving healthcare services and benefiting patients in a more connected and data-driven health system.

1.6 Research Questions

- How can the STRIDE Threat Modelling Framework be effectively utilized to address the identified security challenges and vulnerabilities within the Electronic or Smart Health System (EHS/SHS)?
- How STRIDE Threat Modelling overcome the research gap in securing patient data and healthcare operations in the digital healthcare ecosystem?

1.7 Limitations of the Study

Following are the limitations of the proposed study:

- The study's scope may limit its generalizability to diverse healthcare settings.
- The availability and quality of data on security incidents could impact the study's findings.
- Technological advancements and evolving cyber threats may necessitate updates to recommendations.
- Variability in healthcare regulations across regions may affect the applicability of security measures.
- Budget and resource constraints within healthcare organizations may limit the implementation of security measures.
- The study recognizes the role of human error and behaviour in security incidents, which may not be fully addressed by recommendations.
- While the study primarily focuses on internal threats, external threats from outside entities can also pose significant risks.
- Achieving and maintaining compliance with healthcare regulations may present practical challenges.

- Ethical considerations related to data security and patient consent may require further exploration.
- The study may not fully account for the complexities of interconnected healthcare systems and potential security challenges related to data sharing among healthcare stakeholders.

Acceptable level of assurance of security requires during development of the system that involve security-by-design principles. Threat modelling is important to understand the applicable threats to elicit the security requirements. It can be perform at early stages of development life cycle of system. Similarly, after designing and implementation threat identification system helps companies to elicit the security requirements. But this practice is not widely adaptable to lifecycle of smart healthcare systems. Because most of the time information centric software-based systems are not able to explore the interaction between cyber and physical spaces of cyber physical systems. So, same in smart healthcare systems.

Literature Review

2.1 Introduction

The review of literature in the context of smart healthcare systems, security, and patient data protection reveals various security threats and the applied techniques to mitigate them. This analysis is critical for understanding the existing challenges in safeguarding patient data within the evolving landscape of smart healthcare(El-Bakkouri, Mazri, and Sciences 2020) Smart healthcare systems, leveraging advanced technologies, have revolutionized the healthcare landscape by enhancing patient care, improving diagnostics, and streamlining medical processes. However, with the integration of sophisticated technologies, these systems become susceptible to a myriad of security attacks, posing significant threats to data privacy and system integrity. A significant amount of investigation has already been carried out regarding the danger of assessment procedures in both business and academia.

(Viswanathan, Jayagopal, and Engineering 2021) Highlighted the vulnerability of small and medium-sized businesses (SMBs) to security attacks, primarily because they often lack a dedicated information security department. These businesses face various software threats, categorized into internet-based, web-data servers, web services, and GUI-based threats. To address these challenges, the authors propose implementing threat analysis at an early stage in the software development process. They specifically focus on intrusion detection attacks within the context of a healthcare management system's web application. The severity of these attacks is assessed based on their occurrence within the software development life cycle. The proposed method's outcomes are then compared with the Microsoft STRIDE framework to gain insights into component boundaries, attack ranking, and a better understanding of security threats in the software development and operational processes.

(LaMalva and Schmeelk 2020) Enhanced the security of Android applications, particularly those related to health, by identifying data processing issues. It is provided by the Open Web Application Security Project (OWASP) Mobile Top 10 to ensure secure software development. The results showed that 43.62% of the analyzed applications violated at least one security rule in a significant way. One team used an open-source static analysis tool named MobSF (Mobile Security Framework) to study the security of 200 healthcare-related Android applications. This work is intended to increase security and privacy in mobile applications targeting healthcare.

(Almulihi et al. 2022) Underscored the significant worry from illegal entrance of sensitive clinical records. They stressed that the ripple effect of huge data breaches goes far beyond just customers and shareholders but to organizations tasked with protecting such information. In both of these cases, the danger to privacy and security is considerable, presenting real problems for those responsible for protecting sensitive information. Such a threat was mitigated by strong security practices and continued vigilance, according to the authors. In other terms, it can be said that smart healthcare systems rely too much on Internet of Things (IoT) devices for data collection and communication, as demonstrated by (Rawat et al. 2022). However, these devices often suffer from security vulnerabilities which place patient data at risk. Meanwhile , (Hasan et al. 2022) described that the existence of insider threats was also a well-documented concern disgruntled employees or individuals forced into data breaches. This creates a difficult situation for data protection efforts. An effective strategy for enhancing the quality and availability of healthcare services involves the implementation of Smart Healthcare Systems. However, the integration of wireless networks and intelligent medical devices has introduced new security challenges, including the potential for identity theft, data breaches, and denial-of-service attacks. These vulnerabilities underscore the importance of establishing a secure and reliable smart healthcare system capable of protecting patient data and ensuring the confidentiality of private medical information (Yan et al. 2023).

2.1 Features of attacks

Inaactive attackers are less harmful to the system (Husnoo et al. 2023) as they do not damage devices directly. Instead, they exploit medical equipment through wireless communication, often operating discreetly in the background without the user's awareness. Typically, these attackers collaborate with others to steal information and access devices.

Active attackers position themselves between the sender and receiver, intercepting information from the sender, modifying it without detection, and forwarding it to the receiver. Such modifications can have significant consequences in the medical field, such as altering drug dosages and prescribing the wrong medication, potentially leading to adverse health effects or even sudden death (Sathaye, Noubir, and Ranganathan 2022).

Insider attackers, which could include doctors, receptionists, or nurses, aim to undermine the reputation of the hospital by acting as secret agents for attackers. They may engage in the theft, transmission, or sale of confidential hospital data to harm specific patients' health conditions for political or financial motives. Outsider attackers infiltrate the system using malicious programs such as Trojan horses, viruses, ransomware, spyware, adware, and phishing emails.

These attacks affect computers by attaching to files, browsers, and operating systems. The objective of these attackers is to obtain comprehensive information about the hospital and patients, intending to sell the acquired information on the black market. The primary goal of these attacks may vary, including targeting hospitals, individual patients, small groups of people, or individuals from other nations, driven by motives like political affairs, terrorism, cultural differences, or ethnicity. Harmfulness, in this context, represents a category of attack designed to achieve specific objectives. A brief overview is presented in Table 2.1 below.

Table 2.1: Review of Security in Smart Healthcare System

Reference	Problem	Security Challenges and Vulnerabilities	Proposed Solution
Adeniyi et al. (2023)	Medical information security	Data Breaches	Implement Advanced Encryption
Al-Muntaser et al. (2023)	Cyber security and anomaly detection	Insider Threats	Behavioral Analysis & Anomaly Detection
Hossain et al. (2023)	Securing IOT system for health care	IoT Vulnerabilities	Enhanced Access Control Policies
AbaOud, et al. (2023)	Privacy preservation in healthcare system	Privacy Violations	Federated Learning for Data Privacy
Almousa et al. (2023)	Anti-Spoofing in medical employee's email using machine learning	Phishing Attacks	Email Authentication Mechanisms
Parkavi et al. (2023)	Data breach in the healthcare system: enhancing data security	Data Breaches	Regular Security Audits
Lee (2022)	Unauthorized access	Insider Threats	Identity & Access Management

Scheibne et al. (2022)	Patient data privacy issue	Privacy Violations	Patient Consent Management Systems
Gyamfi and Jurcut (2022).	Security risk	IoT Vulnerabilities	Intrusion Detection Systems
Yeng et al. (2022)	Security attack	Phishing Attacks	Employee Training Programs

In Table 2.1, various security challenges and proposed solutions have been discussed in recent research in healthcare sector. (Adeniyi et al. 2023)Addressed data breaches by implementing advanced encryption, but limitations included limited scalability and resource-intensive processes. Future work suggests investigating block chain technology for improved security. (Al-Muntaser et al. 2023) focused on insider threats and proposed behavioral analysis and anomaly detection. However, they encountered high false positive rates and plan to enhance anomaly detection methods in the future. (Hossain et al. 2023) tackled IoT vulnerabilities with enhanced access control policies, but they faced challenges related to device heterogeneity and interoperability. Their future work aims to develop IoT security standards. (Abaoud, Almuqrin, and Khan 2023) worked on privacy violations using federated learning for data privacy, but faced issues such as communication overhead and data leakage. They plan to investigate differential privacy further. Almousa et al.(2023) dealt with phishing attacks and email authentication mechanisms. Limitations involved user awareness and errors, leading to the exploration of AI-driven anti-phishing solutions. (Parkavi et al. 2023) addressed data breaches through regular security audits but noted incomplete audit coverage, prompting the need for automated audit tools. (Lee 2022)targeted insider threats with identity and access management, though complexities and access policy errors were encountered. Future work involves enhanced policy management. (Scheibner, Ienca, and Vayena 2022) focused on privacy violations and patient consent management systems, highlighting challenges in consent revocation. They aim to advance consent mechanisms. (Gyamfi and Jurcut 2022) worked on IoT vulnerabilities with intrusion detection systems. They faced issues related to false positives and adaptive attacks, leading to a future focus on machine learning-based IDS. Finally, (Yeng et al. 2022) tackled phishing attacks through employee training programs but encountered human errors and evolving threats. They plan to continue training and awareness efforts. These studies contribute to the ongoing efforts to enhance security and data protection in the healthcare sector.

Various security threats, including spoofing attacks, tampering attacks, repudiation attacks, information disclosure attacks, denial of service (DoS) attacks, and privilege elevation attacks are particularly focused by the researcher in the context of smart health care system (Abughazaleh, Bin, and Btish 2020). By utilizing the proposed framework, healthcare organizations can identify and prevent these threats, ensuring the protection of patient data, data integrity, and system availability. It empowers healthcare systems to proactively strengthen their security measures and maintain the integrity of healthcare operations.

Smart healthcare systems, leveraging advanced technologies such as the Internet of Things (IoT) and artificial intelligence (Thabit et al. 2020) has witnessed significant advancements in recent years. As these systems evolve, the security and privacy of healthcare data become paramount concerns.

To execute privacy-based attacks, attackers aim to acquire private or confidential patient information from external sources like staff nurses, doctors, and receptionists. These attacks typically fall under the category of In-Active attacks.

The security goals of the SHS system encompass logical SHS security, data protection, system protection, device protection, and user-related security aspects. These goals include data confidentiality, integrity, and availability, as well as privacy, user authentication, system integrity, system authentication, and system availability.

Above reviewed literature helps to design the following hypothesis:

H1: How can the STRIDE Threat Modelling Framework be effectively utilized to address the identified security challenges and vulnerabilities within the Electronic or Smart Health System (EHS/SHS)?

2.2 Privacy Attacks

Tapping Communication Attack: Executed through mobile communication, this attack involves spying on communication using powerful tools, collecting information to compromise privacy.

- Man-in-the-Middle Attack: Occurs due to weak encryption in wireless access points, allowing unauthorized access to medical devices. Attackers may attempt to control devices, leading to potential modifications in drug dosage and resulting in health issues for patients.

- Data Trapping Attack: Damages medical data and secret information through interception, exploiting weak encryption in wireless communication. Tools like TCP dump and Network Miner can be used for data trapping.

- Surveillance Attack: Involves tapping telephone communications to intercept information, relying on incoming or outgoing calls for unauthorized access.

This attack is aimed at hacking and tracking patient data by medical devices, identifying their home or workplace to collect basic and personal information. To enhance security, patients are advised to utilize virtual private networks, periodically changing their IP addresses and MAC addresses using proxy servers.

The above discussion helps in designing the hypothesis that addresses the second research question and demonstrate the importance of mitigating the patient data privacy issues in SHS.

H2: How STRIDE Threat Modelling overcome the research gap in securing patient data and healthcare operations in the digital healthcare ecosystem?

While the existing literature provides valuable insights into various aspects of smart healthcare system security and data privacy, a notable research gap persists. The majority of studies focus on technical solutions, such as encryption, authentication, and anomaly detection. However, there is a limited exploration of the socio-ethical dimensions, user perceptions, and the impact of security measures on the overall user experience in smart healthcare systems. Future research should aim to bridge this gap by incorporating a multidisciplinary approach that considers both technical and human-centric aspects, fostering a holistic understanding of the challenges and opportunities in securing smart healthcare systems.

Summary

The proposed work aim is to build upon and enhance the existing body of work in smart healthcare systems, as outlined in various surveys, with a particular emphasis on addressing security and privacy concerns. The ultimate goal is to contribute to a comprehensive knowledge base regarding security and privacy in SHS, benefiting future researchers and professionals engaged in this domain.

In this chapter, we provide several key perspectives regarding why security and privacy are extremely important for a smart healthcare system. The first of which shows that, because the healthcare sector directly effects individual healthiness, we are able to obtain evidence on one area where cyber malevolence really counts — making a clear and compelling case for why securing this key environment necessitates greater attention in research. In addition, existing literature focused on threats and security mechanisms but there are few discussions regarding the detailed security requirements as well as patient safety; third, a lack of research exists on the overall healthcare model design as well as identification of key stakeholders, core ingredients/content and technologies. Lastly, while multiple works discuss threat taxonomies in the healthcare domain; aligning with common threat frameworks for ensuring compliance and interoperability to other efforts is disregarded.

Proposed Methodology

3.1 Introduction

Introduce a methodological framework addressing the challenges of securing patient data in smart healthcare systems. Grounded in the STRIDE threat modelling framework, the methodology systematically identifies and mitigates security threats. The research model encompasses key components like hypothesis formulation, research methodology, and performance measures, providing a comprehensive blueprint. This proposed approach is primarily focused on maximizing adaptability and scalability for future technology developments in the healthcare sector. Using Microsoft Threat Modeling Tool 7.3, software organizations can enhance the security posture of software applications by systematically identifying threats and vulnerabilities in all stages of the development lifecycle. Threat modelling is essential to the domain Smart Healthcare Systems (SHS), as it involves a combination of advanced technologies, which gives rise to security threats. The technical examination will test the accuracy of Microsoft Threat Modeling Software in identifying threats within SHS with a further analysis using a Data Flow Diagram of the system.

3.2 Tools: Microsoft Threat Modelling Tool vs: 7.3

The following are the steps of proposed model:

- **Visual Representation:**

Smart Healthcare Systems (SHS) and vision representation of attack surface with Microsoft Threat Modeling Software. Although there could be spacer code introduced to make it easier for comprehension and communication, this picture tells a story: Make sure you can identify potential security threats by learning more about the process, in order that you will understand better what happens on global platforms; also how safe (or unsafe) they are.

- **Data Flow Diagram (DFD):**

Data Flow Diagram (DFD), used to illustrate the functional behavior of data as it moves within Smart Healthcare Systems (SHS) [] MICROSOFT THREAT MODELING SOFTWARE // DFDs help diagram the data flow among various stakeholders, enabling a higher level of visualization to identify where the system could be possibly vulnerable or compromised.

- **Identifying Threats:**

It then uses a threat library with documented threat scenarios and attack patterns. The tool assists in methodically identifying potential risks of data storage, transmission, and processing by correlating these threats with the Data Flow Diagram (DFD) of the SHS.

- **Attack Surface Analysis:**

Microsoft Threat Modeling Software helps to find out attack surface of Smart Healthcare Systems (SHS) where it point our entry points, trust boundaries and potential vulnerabilities. It is critical to examine all these security problems for the threat model process, which needs to be comprehensive.

- **Integration with Development Process:**

Developers can quickly introduce security concepts at the design stages of development lifecycle, as this software easily integrates with the SLC. Such an approach is proactive in nature and greatly reduces the risk of infusing vulnerabilities while coding and testing.

- **Mitigation Recommendations:**

The tool not only identifies threats but also provides mitigation recommendations. This enables development teams to prioritize and implement security controls effectively; addressing potential vulnerabilities before they can be exploited in a real-world scenario. Efficient resource allocation to prioritize the security efforts in smart healthcare systems in limited budget is required. Besides its smart health care systems are strictly bound to follow the security and privacy regulations. Data protection compliance. Following is the detail of proposed methodology.

3.3 Proposed Methodology

The research methodology involves a systematic process of threat identification to mitigate security and patient data privacy via STRIDE framework. It enhanced the security and data privacy in smart healthcare systems. Mitigation strategies are proposed based on the STRIDE analysis, guiding the implementation of measures to safeguard assets. The model emphasizes continuous monitoring, staff training, compliance with regulations, and transparent communication to ensure a robust security posture aligned with privacy considerations. All security frameworks focus on threat identification. Threat modelling is a structured approach for identification, quantification and prioritization of security and data privacy risks in a system. threat modelling proactively helps in identifying and addressing the potential security risks before exploitation of the system by any malicious actors. Generally, literature comes up with generalizing the process of threat modelling in three basic steps shown in Figure 3.1

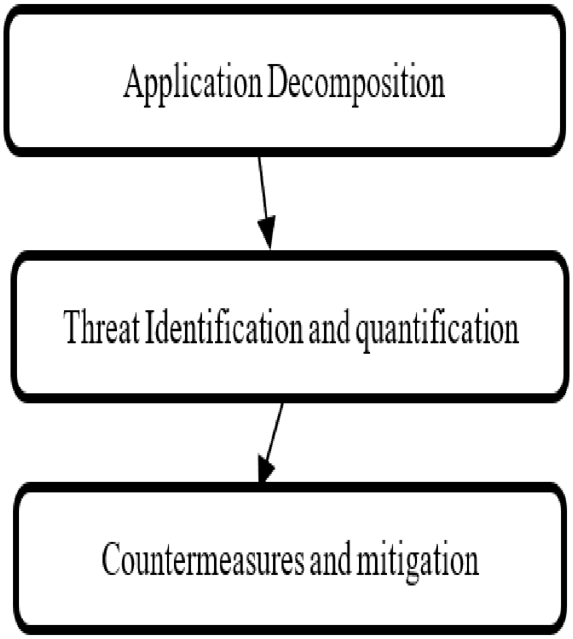
Application Decomposition
Threat Identification and quantification
Countermeasures and mitigation

Figure 3.1 : Main Steps of Process

1. Application breakup – Stage 1 is about acquiring information about the system and converting it into a data flow diagram (DFD).

2. Threats are identified and categorized based on the threat model, e.g. STRIDE the subsequent step is to get the risk verified in a risk evaluation model (DREAD, for example), and then he derives an expression ⟼ the risk in it with severity which we can model as so:

Risk = Likelihood of Outcome x Impact (1)

3. Implementation of countermeasures and mitigation - Identify countermeasures, and establish the current state of their mitigation (non-mitigated, partially mitigated or fully mitigated).

4. Control principles Identification and assessment of threats are identified and categorized based on the threat model, e.g. STRIDE The subsequent step is to get the risk verified in a risk evaluation model (DREAD, for example), and then he derives an expression ⟼ the risk unit With severity which we can model as so:

Risk = Likelihood of Outcome x Impact of that outcome (2).

3.4 Research Methodology

Input: Assets within the smart healthcare system (e.g., patient health records, medical devices, communication channels).

Output: Improved security and data privacy through the application of the STRIDE framework.

Step1:

- Outline the smart healthcare system scenario
- Discuss the case study scenario

Step2: Asset Identification

- Identify and categorize assets (i.e. informational & physical) within the smart healthcare system. Include patient health records, medical devices, and communication channels in the asset inventory.

Step3:

- Threat Identification via STRIDE framework
- Conduct a systematic analysis to identify potential threats using STRIDE.

Step 4: Rank threats via Dread Analysis

Apply the STRIDE framework to analyze each identified threat. Consider Spoofing, Tampering, Repudiation, Information Disclosure, Denial of

Service, and Elevation of Privilege for each threat. Following the completion of the STRIDE analysis, proceed with a DREAD analysis for individual threats to quantify and prioritize those using DREAD criteria. Allocate numerical values to each DREAD aspect to facilitate a quantitative evaluation of threat severity.

DREAD_Score = (Damage+ Reproducibility+ Exploitability+ Affected_Users+ Discoverability)/5

Step 5: Mitigation Strategies

Propose mitigation strategies for each identified threat based on the STRIDE analysis. Include technical controls, policy enhancements, and user education to address vulnerabilities.

Step 6: Combined Mitigation Strategies

Create strategies to mitigate identified threats by taking into account findings from both the STRIDE and DREAD analyses. Give priority to mitigation actions based on severity scores derived from the DREAD analysis, with a primary focus on addressing threats with higher-risk levels at the forefront.

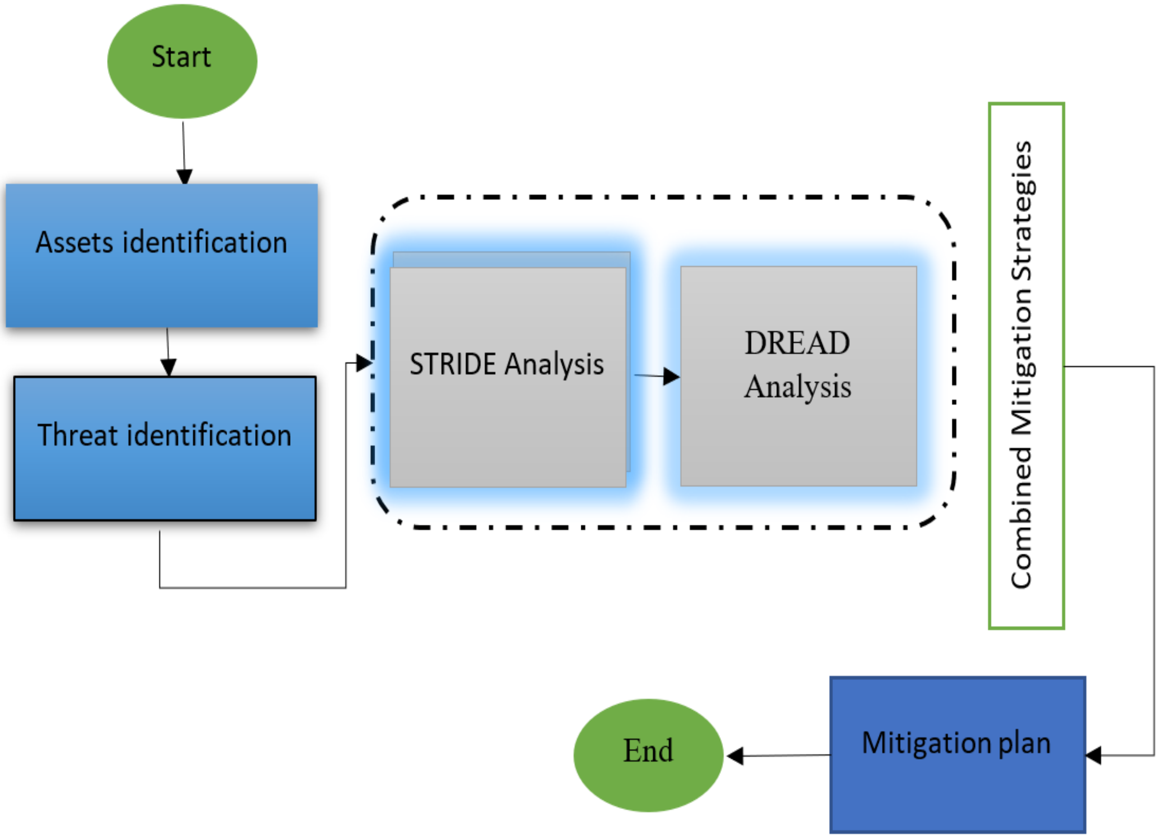

Figure 3.2: Proposed Research Model

Scenario and Asset Identification

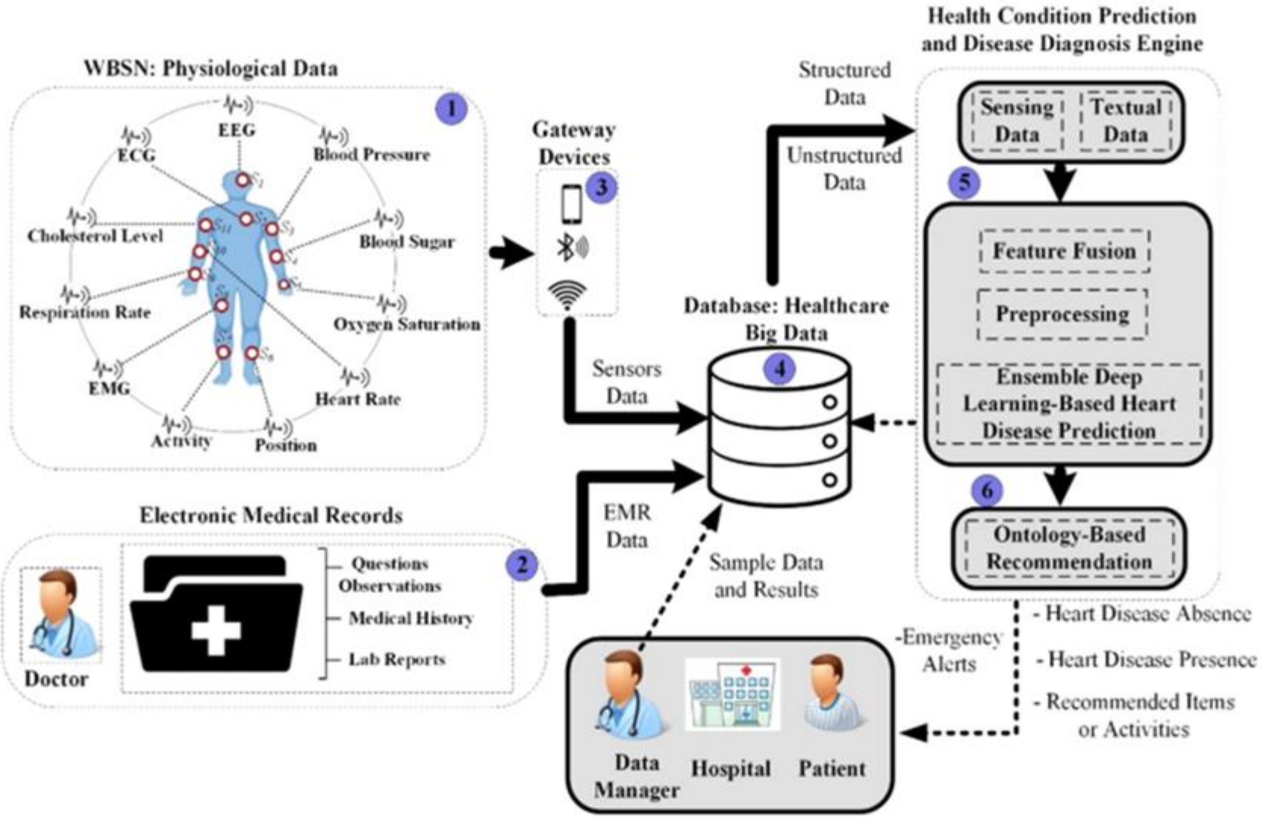

Figure 3.3: SHS Scenario

The system details are derived from this case study in which scenario depicts the most generic SHS. Patients utilize Bluetooth-enabled medical IoT devices, such as blood pressure monitors, glucose meters, and wearable fitness trackers, within the comfort of their homes. These devices continuously gather health metrics, feeding the data into the central database. Similarly, data from EMR system is transferred to this central database. Further this data is distributed to analytical machine or diagnosis engine or system to generate health or emergency alerts. On the same time the central database is accessible to different stake holders as well as shown in the above Figure 3.3. This is the most general and suitable scenario chosen from literature to propose a methodology for early detection of security threats and data privacy issues via STRIDE framework.

The data flow of SHS is decomposed in Figure 3.4 to get better understanding of working of the system. It helps in eliciting the threats points and data privacy issues clearly.

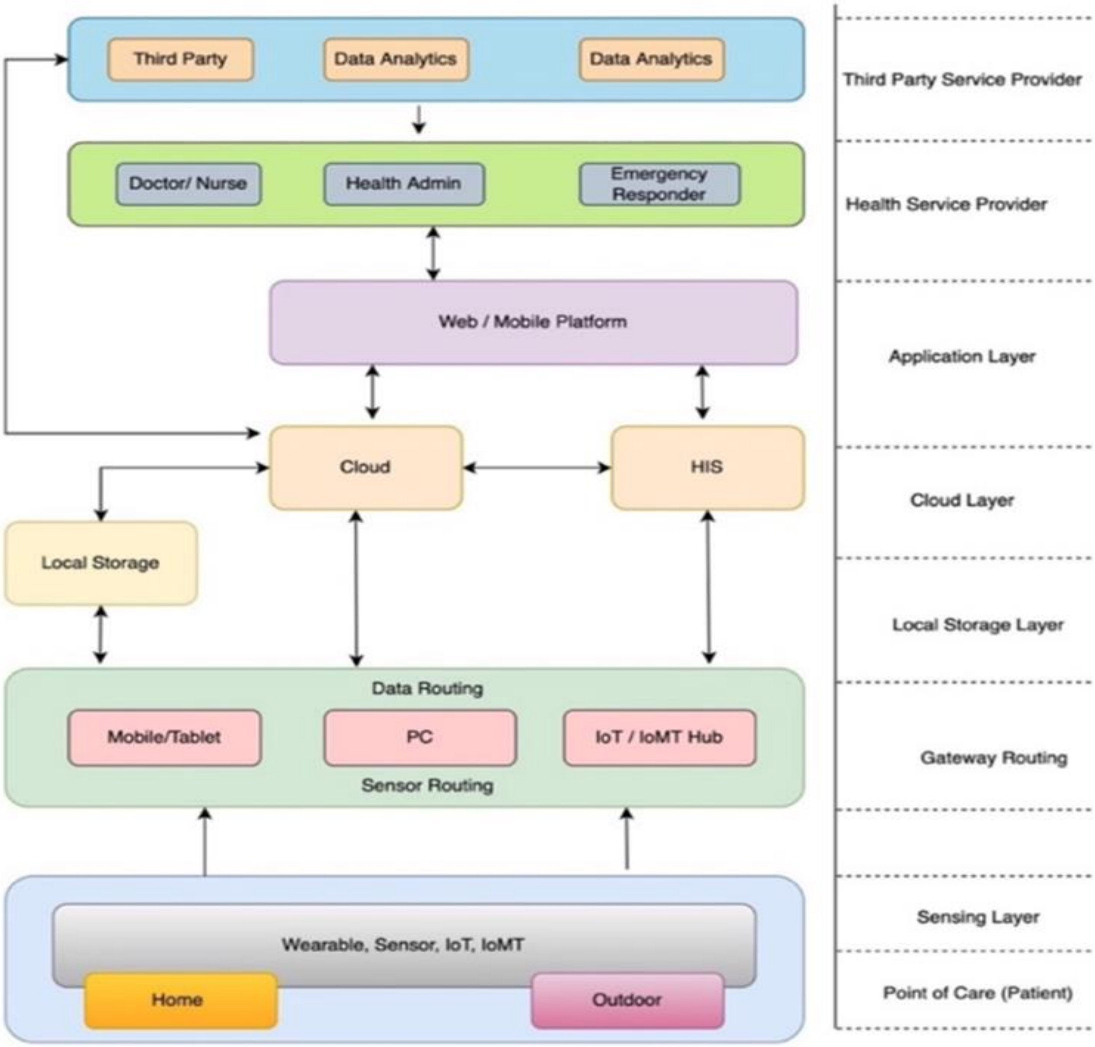

Figure 3.4: Decomposition of a Sscenario

3.5 Asset Identification

3.6.1 Informational Security in Smart Healthcare Systems:

Informational security is a critical aspect of smart healthcare systems, ensuring the confidentiality, integrity, and availability of sensitive health data. As these systems increasingly rely on digital technologies, the protection of patient information from unauthorized access, disclosure, or tampering becomes paramount. Several key components contribute to the informational security framework in smart healthcare:

Utilizing robust encryption protocols for data in transit and at rest safeguards patient information from interception or unauthorized access. In the smart healthcare ecosystem, it's essential that data exchanged between devices, applications and databases are all sensitive health data — securing its should use advanced encryption algorithm.

Authentication Mechanisms: Implementation of strong authentication mechanisms like biometrics, multi-factor authentication and secure login credentials ensures the identity by users accessing the smart healthcare system. This ensures that only the authenticated individuals can access patient data, blocking others.

Access Control Policies: Defining your access control policies will establish an order in which well-stipulated roles are given to various users connected with the smart healthcare system. Although role-based access control (RBAC) and attribute-based access control (ABAC) mechanisms prevent any user from gaining unauthorized access by restricting users to the information required for their roles.

Routine Security Audits: To regularly perform security audits and vulnerability assessments to see if there are any vulnerabilities that need fixing. This includes regular access log reviews, checks of system and user settings that are known to create security vulnerabilities as well as common sense monitoring to detect activities which indicate some kind of malfeasance.

Incident Response Planning: Strong incident response planning trains healthcare organizations on how to be prepared for what is about to happen and ready their teams take prompt action. Rapid recognition of security incidents, and containing, eliminating or recovering from those attacks are essential actions to mitigate the effects on patient data.

Physical Security on Smart Healthcare Systems: Information security is now essential to the blend, and physical protection works in tandem keeping with the need for end-to-end security when it comes to devices themselves as well as every part of E2E entities touch. Physical security concerns must be addressed to prevent unauthorized physical access and tampering, which could compromise the healthcare environment integrity:

Physical Access Control Systems: Physical access control systems such as biometric scanners, keycard readers and video surveillance cameras limit entry to areas like data centers, server rooms or medical storage facilities. Such measures protect the healthcare infrastructure from being physically tampered with by unauthorized personnel.

Facility Design: By incorporating security features such as placement of security cameras and controlled entry points in healthcare facility designs or closed/secured storage areas for medical devices at the clinic/hospital/wards minimizes unauthorized access.

Environmental Controls: Ensuring that the environment is set up so healthcare equipment works how it was meant to medical equipment and server rooms These devices are being used as/ in the server rooms or to control temperature, humidity and other environmental conditions anywhere medical equipment is stored.

Inventory/Asset Management: Deploying complete inventory/asset management systems, which helps in tracking and monitoring the devices/equipment inside facilities of healthcare. This reduces the risk of theft and increases safety, as lost or unauthorized devices can be quickly found.

Training and Awareness: Healthcare personnel to be taught about physical security measures. Training programs should educate staff about the need to report any suspicious activities and follow security protocols.

Smart systems of healthcare could be merging strong informational as well as physical safety measures constructing offshore shield in contradiction to the digital along with a bodily threat confirming data patient dignity besides the sanctity of health care operations.

3.6 Threat Identification and Risk Assessment

3.7.1 Smart Healthcare System and STRIDE Framework

Especially, with reference to the model formulated for the threats faced by a smart healthcare system STRIDE is useful for identifying and characterizing threats. The following is how the STRIDE categories map with this space.

Spoofing: Spoofing refers to gaining unauthorized access into patient records by pretending to be a healthcare provider.

Tampering: Unauthorized alterations to medical data may result in misdiagnosis and hence perilous.

Non-repudiation: If actions performed in the system are subsequently denied this could affect traceability making it hard to hold someone accountable when they deny responsibility.

Information Disclosure: The risk of unauthorized users gaining access to sensitive patient information is one of the most significant.

Denial of Service: A disruption to critical healthcare services that could affect patient care and safety.

Elevation Of Privilege: Escalation Privilege escalation by unauthorized elevation of privilege, unearthing right against secure boundaries.
Besides that, DREAD framework is used to the severity of identified threats in a smart healthcare system. It assesses these dimensions;

Level of Damage (D): Evaluation of the consequences if a threat occurs, what will be the result on patient files or essential medical services.
An attack (R): How easy it is to perform the action that exploits a weakness?

Exploitability (E): How easy it is for an attacker use this vulnerability, such as technical prowess or means needed.
Affected Users (A): Helps in understanding how big the threat is, whether it affects individual patients, healthcare providers or the entire system.

Discoverability (Di): This is how much the vulnerabilities that can be exploited in order to perpetrate an attack are difficult to detect, even if high / low response time or effective probability.
Thus the methodology guarantees a structured way of identifying, classifying and evaluating threats by including these frameworks. Thus, allows securing the smart healthcare environment by implementing dedicated and tactical security controls.

3.7 Threat Modelling

This is done through the use of the Microsoft Threat Modeling Tool and proves to be very useful when using it in SHS. This provides developers a systematic way to proactively surface potential threats and vulnerabilities in the initial stages of SHS development, by using this framework. Building up this kind of inventory is the foundation to enable a later use of DREAD model to rate each threat across five metrics, including damage potential, reproducibility, exploitability, affected users and discoverability. Through this disciplined approach, both security concerns are identified and a roadmap is engineered early in the development lifecycle to enable robust security measures within the Smart Health System.The integration of the Microsoft Threat Modelling Tool and the STRIDE framework offers a systematic and comprehensive approach to threat identification and mitigation, thereby enhancing the overall security resilience of Smart Health Systems.

Summary

Chapter demonstrate a complete proposed methodology based on STRIDE framework following all steps discuss in proposed methodology. The smart healthcare scenario discussed in this work is already published, and its DFD is comprehensively drawn using Microsoft threat modelling tool to identify the threats results are discussed in Chapter 4. Figure 4.1 is the representation of decomposition of the scenario in layers that help in drawing the flow from one component to another become easy and helps in identifying the threats more easily.

Results and Discussion

4.1 Introduction

Results of threat identification and data privacy are discussed in detail. In this chapter, the utilization of the STRIDE framework, facilitated by the Microsoft Threat Modelling tool, is examined as a comprehensive approach to identify and analyse potential threats within the system, providing a nuanced understanding of the security landscape. DREAD is applying for risk assessment.

4.2 Data Flow diagram

Having enumerated all the assets, our objective is to visually represent the trajectory of data through the device and application. Having multiple routes for data sharing or travelling it emphasizing its processing routes. The following graphical representation serves to simplify the documentation of potential vulnerabilities and threat points within smart healthcare system. The main intent behind presenting the smart healthcare system was to understand the data flow among various components of the system to cater both technical and non-technical stakeholders. Following Figure 4.1, presented scenario is delineate i.e. smart healthcare system wherein a health device transmits health records or sensor readings to connected central database using different gateway devices. This application encrypts and subsequently transmits the data to the database which not only analyses it but also disseminates the forecasting to healthcare providers while storing it in the database medical data.

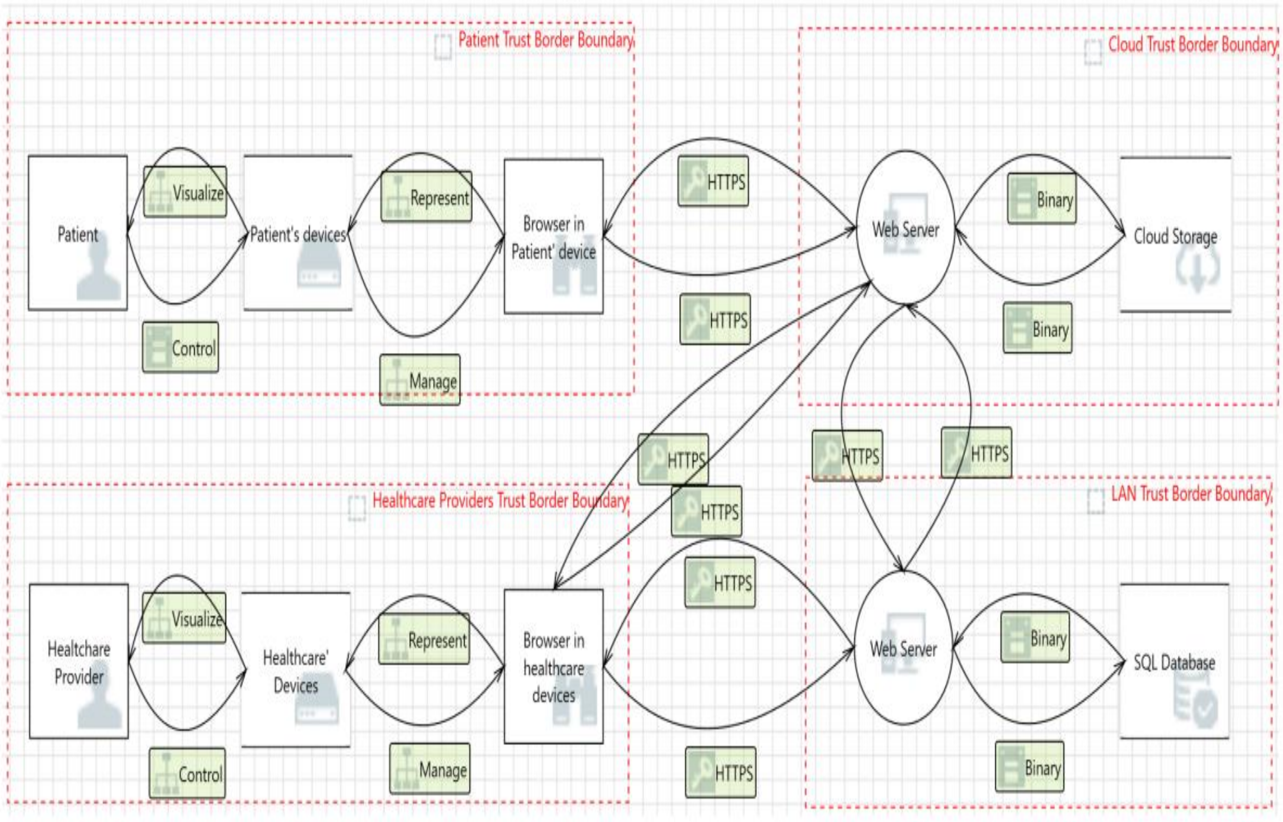

Figure 4.1: DFD of SHS Scenario

Figure 4.1 presents the data flow very clearly and, even for moderately technical users, will help in identifying possible threat points much faster. The sections of a system from which other systems, users or data is trusted (i.e., trust boundaries) are very important in threat identification when using Data Flow Diagrams (DFD). These boundaries mark where transitions of data occur between trust levels, helping greatly in understanding and reviewing security of a system. Identifying trust boundaries is critical to uncover vulnerabilities and ascertain security threats, such as unauthenticated access or data tampering.

For example, consider a smart healthcare system. One example of this type of trust boundary is between a user interface where patients enter their information and the back-end server that handles storing and processing that data. Ensuring the data security while it passes through this security barrier is indispensable to prevent unauthorized access.

By explicitly defining trust boundaries patient trust border boundary, healthcare providers trust border boundaries, cloud and land storage trust boundaries in a DFD, security analysts can systematically analyze data flow, identify potential vulnerabilities or threats, and implement effective security measures to fortify these critical junctures. This concept is integral to the practice of threat modelling and risk assessment, contributing to the overall enhancement of a system's security.

4.3 STRIDE Threat Classification

Following table shows the threat classification under Stride framework. This classification help to identify the threats in SHS case study.

Table 4.1: STRIDE Threat Classification

Threat Classification	Cause	Desired Property	Affected Attribute of Smart Healthcare Systems (SHS)
Spoofing and Tempering	Examination of authentication processes, such as username/password systems. Evaluation of the accuracy of information and software managing patient data and healthcare services.	Strong authentication measures to ensure authenticity. Integrity through techniques like hash functions and checksums.	Connectivity, Data accuracy and Reliability, Data security and privacy, Integration with Healthcare systems, Health data privacy and security, Health Insights and Analysis, Remote Healthcare support, and User-friendly Interfaces.
Repudiation	Implementation of tools to detect and document user activities, such as audit trails and digital signatures.	Non-repudiation through techniques like audit trails for irrefutable proof.	Data Accuracy and Reliability.
Information Disclosure	Regular vulnerability assessments and penetration tests.	Confidentiality using safeguards like encryption, access controls, and data masking.	Connectivity, Data privacy security, Integration with the Healthcare Systems, Health data privacy security, Health Insights and Analysis, Remote Healthcare and support, Specific medical applications.
Denial of Service (DoS)	Monitoring network traffic and system performance for unusual behaviour.	Availability through redundancy and failover procedures.	Connectivity and Remote Healthcare support.
Elevation of Privilege (EoP)	Enforcing stringent access controls and role-based permissions.	Authorization through strict control of user privileges.	Connectivity, Data privacy and security.

DOS ,and elevation of privilege for given scenario with a detail demonstration covering under what cause trigger it , which component of the system get effect and what is the desired step. Following table shows the list of threats identify after applying STRIDE in Microsoft Threat Modelling Tool 7.3.

Table 4.2: Result of Threat Identification

Threat Number	Threat Name	STRIDE Category	Description
T-1	Unauthorized Access	EoP	Illegal actions to access data
T-2	Data Breaches	Information disclosure	Privacy of patient's data compromise
T-3	Device Tampering	Tampering	Adversary Threats due to exploiting the monitoring devices or logs without appropriate access.
T-4	Denial of Service (DoS) Attacks	Denial of Service	Hacker intentionally overwhelms the system to show it busy
T-5	Ransomware	Tampering	Encrypting data on the device and demanding a ransom.
T-6	Malware and Viruses	Tampering	Caused by malicious software that compromising working of the the device.
T-7	Man-in-the-Middle Attacks	Information Disclosure	Capturing sensitive data by interception the communication or network.

T-8	Data Interception and Eavesdropping	Information Disclosure	Capturing sensitive data transmitted via Bluetooth.
T-8	Interoperability Issues	Information disclosure	Risks from diverse device and system integrations.
T-9	Privacy Violations	Information disclosure	Illegal sharing or data collection
T-10	Device Malfunction	DoS	Faults in tangible devices
T-11	Data Integrity Issues	Tampering	Manipulation leading to wrong diagnoses or treatments.
T-12	Inadequate Encryption	Tampering	Threats due to lack in privacy caused by weak encryption
T-13	Insufficient Logging/Monitoring	Repudiation	Threats caused by humans illegal or malicious actions
T-14	Lack of Physical Security Measures	Spoofing	Inadequate security of network or physical devices
T-15	Social Engineering	Spoofing	Manipulating individuals for unauthorized access.
T-16	IoT Botnets	DoS Attack	Botnet devices cause threats
T-17	Data Retention/Disposal	Information disclosure	Not properly handling data during retention or disposal

Table 4.3: Threats identify via STRIDE

Range	Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability
1	No harm	Almost impossible	Almost un feasible	Almost None	Nearly impossible
2-3	Minor damage	Very specific condition	High expertise needed	Small Subset	Great difficulty
4-5	Moderate damage	Occasionally with efforts	Moderate efforts	Moderate number	Some effects and tool
6-7	Significant damage	Often some conditions	Common tools	More than half	Relatively easy
8-9	Major damage	Almost Always	Easily with minimum knowledge	Most users	Very easy
10	Catastrophic damage	Every time	Almost no effort	All users	Completely obvious

The STRIDE framework applied in the Microsoft Threat Modelling Tool revealed a comprehensive set of threats within the Smart Health System. These threats span various categories, including unauthorized access, privacy breaches, adversary actions, and human-related risks. Notable threats include unauthorized users gaining elevated access (T.1), data breaches leading to patient data disclosure (T.2), device tampering through unauthorized changes (T.3), and denial of service attacks overwhelming system functionality (T.4). The framework also identified risks such as ransomware attacks encrypting data (T.5), malware compromising devices (T.6), and insider threats causing harm (T.10). The results highlight the diverse nature of threats and count 26 threats, emphasizing the importance of addressing each category to fortify the security of the Smart Health System.

4.4 DREAD Risk Assessment Model

Following table shows the range of DREAD. Utilizing this range the risk assessment of SHS is performed results are shown in Table 4.4

Table 4.4: Risk Assessment Model

Sr. No	Threads identity via STRIDE	Count
1	Spoofing	5
2	Tampering	7
3	Repudiation	1
4	Information Disclosure	6
5	Denial of Service	3
6	Elevation of Privilege (EoP)	4
	Total threat Count	26

Table 4.5: Results of Risk Assessment using DREAD

Threat Number	Threat Name	STRIDE Category	D
T-1	Illegal Access	E	7
T-2	Data Fissures	I	9
T-3	Device Interfering	T	8
T-4	Denial of Service (DoS) Attacks	D	9
T-5	Ransomware	T	10
T-6	Malware and Viruses	T	8
T-7	Man-in-the-Middle Attacks	I	7
T-8	Data Intervention and Eavesdropping	I	8
T-9	Firmware Liabilities	S	7
T-10	Threats form inside the organization	E	8
T-11	Physical Security Breaches	S	9
T-12	Software Vulnerabilities	T	8
T-13	Insecure Communication	T	7
T-14	Lack of Authentication/Authorization	E	7
T-15	Weak Passwords	E	6
T-16	Lack of Updates/Patches	S	8
T-17	Interoperability Issues	I	7
T-18	Privacy Violations	I	9
T-19	Device Malfunction	D	8
T-20	Data Integrity Issues	T	8
T-21	Inadequate Encryption	T	7
T-22	Insufficient Logging/Monitoring	R	7
T-23	Lack of Physical Security Measures	S	9
T-24	Social Engineering	S	9
T-25	IoT Botnets	D	8
T-26	Data Retention/Disposal	I	7

The risk assessment analysis based on the DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) scores reveals the varying levels of risk associated with identified threats in the system. Unauthorized Access (T.1) poses a moderate risk with a DREAD score of 5.2, indicating potential unauthorized access but with a relatively moderate impact. Data Breaches (T.2) present a higher risk with a DREAD score of 7.4, signifying a critical concern due to the significant impact of unauthorized access leading to the disclosure of patient data. Device Tampering (T.3) is of moderate risk (DREAD 6.4), reflecting concerns about unauthorized physical or software changes to the device. Denial of Service Attacks (T.4) carry a considerable risk (DREAD 7.4) due to the potential disruption of device functionality. Ransomware (T.5) represents a high risk (DREAD 8.8), emphasizing the severe consequences of encrypting data and demanding a ransom. Malware and Viruses (T.6) pose a significant risk (DREAD 7.8) with the introduction of malicious software compromising the device. Man-in-the-Middle Attacks (T.7) present a moderate risk (DREAD 6.4), impacting Bluetooth communications. Data Interception and Eavesdropping (T.8) show a substantial risk (DREAD 7.2), particularly concerning privacy issues. Firmware Vulnerabilities (T.9) carry a moderate risk (DREAD 5.8) related to potential exploitation. Insider Threats (T.10) pose a moderate risk (DREAD 6.8) associated with actions by individuals with access. This comprehensive analysis guides the prioritization of mitigation efforts, allowing for a focused approach to address the most critical security concerns within the system.

4.5 Countermeasures

Considering above discussion, the following counter measures can adopt to mitigate the secret. Considering above discussion, the following counter measures can adopt to mitigate the security and patent data privacy issues.

Table 4.6: Counter Measures

Threat Number	Threat Name	STRIDE Category	Counter Measure
T-1	Unauthorized Access	E (Authorization and Access Threats)	Implement strong access controls, such as multi-factor authentication, to limit unauthorized access. Conduct frequent audits and monitoring of user permissions to verify compliance with least privilege principles.
T-2	Data Breaches	I (Privacy Threats)	Utilize strong encryption protocols to secure patient data both during transmission and storage. Implement strict access controls and user authentication mechanisms to restrict unauthorized data access. Conduct regular security audits to identify and address potential vulnerabilities proactively.
T-3	Device Tampering	T (Adversary Threats)	Incorporate physical security measures like tamper-evident seals and secure enclosures to discourage and identify unauthorized physical access or alterations to devices. Employ secure boot processes to mitigate unauthorized software modifications.
T-4	Denial of Service (DoS) Attacks	D (Adversary Threats)	Implement network and traffic monitoring systems and preventive measure storesist DOS attacks. Build redundancy and load balancing in order to keep your service up even when attacked
T-5	Ransomware	T (Adversary Threats)	Regularly back up essential data and create an effective plan for retrieving the data. Always have reliable antivirus and run the system scan at regular intervals to find out & remove malware. Teach your users how to recognize and avoid potential ransomware.
T-6	Malware and Viruses	T (Adversary Threats)	Keep all of your software and antivirus programs

			up to date with security patches. Teach users the best practices of browsing safely – avoid downloading or opening files from 'unverified' sources. Adopt network-based security methods to alert and block malware.
T-7	Man-in-the-Middle Attacks	I (Adversary Threats)	Use strong encryption protocols such as SSL/TLS for Bluetooth communication to prevent snooping and interception. Use the right authentication and safe authentication for both connecting devices in order to identify them. Communications protocols should be updated and patched as necessary to address known vulnerabilities;
T-8	Data Interception and Eavesdropping	I (Privacy Threats)	Utilize robust encryption protocols for securing Bluetooth communications. Implement secure channels and sockets to ensure the confidentiality and integrity of data transmission. Conduct regular monitoring and audits of communication channels to detect and address any indications of unauthorized access.
T-9	Firmware Vulnerabilities	S (Adversary Threats)	Always keep the device firmware up-to-date so that known vulnerabilities are reduced. Follow secure boot protocols and keep firmware updates signed to protect against corruption. If needed, you can add code integrity checks to detect and prevent unauthorized changes.
T-10	Insider Threats	E (Human Threats)	Implement role-based access controls and perform user permission review on a regular basis. Train employees on security with greater emphasis being placed on the associated risks of insider threats. Keep track of user behaviour including the deployment of log variants to identify and neutralize any malicious activity in real-time.
T-11	Physical Security Breaches	S (Human Threats)	Enforce physical barriers and place surveillance cameras and access controls to prevent unauthorized physical entry. Provide staff training on the enforcement of security protocols and create a vigilance where all employees are encouraged to alert administrators to unusual activity
T-12	Software Vulnerabilities	T (Adversary Threats)	Regularly update and patch software to reduce the likelihood of exploitation.
T-13	Insecure Communication	T (Privacy Threats)	Use appropriate security protocols with strong

			encryption methods
T-14	Lack of Authentication/Authorization	E(Authentication Threats)	Enable multi-source or multi-level authentication
T-15	Weak Passwords	E(Authentication Threats)	Password Complexity Standards and Mandatory Periodic Password Resets Educate password strength and disallowed simple words Set up account lockout policies to discourage brute-force attacks.
T-16	Lack of Updates/Patches	S (Adversary Threats)	Enable regular updates of system. It avoids security issues.
T-17	Interoperability Issues	I (Privacy Threats)	Define standard communication protocols so that the devices and systems can smoothly integrate. Before you start to implement new integrations, try compatibility tests oh! Part (c) Regular review of the integration and updating relevant mechanisms to mitigate any compatibility problems
T-18	Privacy Violations	I (Privacy Threats)	Design privacy violation polices and literate the employees to avoid violation.
T-19	Device Malfunction	D (Adversary Threats)	Add redundancy and fault tolerance to mitigate the impact of possible hardware failures. Frequent monitoring — Keep an eye on the health and performance of devices to catch signs of trouble sooner rather than later.
T-20	Data Integrity Issues	T (Adversary Threats)	Add the encryption controls to protect data in motion and at rest. Use checksums, and hash functions to identify alterations in data due to unauthorized interventions. Regular audits of data integrity safeguards to identify potential issues — and then prioritize fixing them.
T-21	Inadequate Encryption	T (Privacy Threats)	Implement strong encryption mechanisms for transmitting as well as storing the data Gruely update protocols for encryption and periodically check if the function of data protection from vulnerabilities. Regular penetration testing to search for the presence of vulnerabilities in your encryption mechanisms.
T-22	Insufficient Logging/Monitoring	R (Human Threats)	Implement extensive logging to record user actions and system events extensively. Perform ongoing monitoring and analysis of logs to combat malicious activities efficiently. Six Critical Things To Do Before You Start Using

			Sudo: Deploy real-time monitoring to detect alerts immediately and fix any potential security incident as they happen.
T-23	Lack of Physical Security Measures	S (Human Threats)	Physical access: Access controls (including physical controls) and surveillance measures to discourage unauthorized physical attacks Conduct regular security training with your staff, especially when it comes to following physical security standards.
T-24	Social Engineering	S (Human Threats)	Maintain security awareness training by keeping these employees up to date on social engineering methods Implement a procedure for identifying people requesting access to sensitive information. Email Filtering and User Authentication: Use detection to defeat risks of Phishing.
T-25	IoT Botnets	D (Adversary Threats)	Implement network segmentation to isolate IoT devices from critical systems. Regularly update and patch IoT device firmware to address known vulnerabilities. Monitor network traffic for signs of botnet activity and respond promptly to any identified threats.
T-26	Data Retention/Disposal	I (Privacy Threats)	Establish clear data retention policies, ensuring compliance with privacy regulations. Regularly review and dispose of unnecessary data in accordance

4.6 Discussion

After drawing the data flow that is provided by the Microsoft Threat Modeling Tool, we automatically generated 90 threats. Actually had one new and important threat not found in attack tree denial of service diagram. Process flow diagram did not reveal new threats. However, it also served as an important tool for visualization of user interaction with the system. One difference between threats identified by the attack tree and the flow diagram as generated also lies in their scope. The attack tree diagram identifies threats for the entire system, but in Microsoft Threat Modeling Tool one exercises each element separately; thus it generates specific threats only for these two components This gives more technical information about where the threat can befall in the system, but also tends to generate many redundant threats (this could actually be mitigated with a single solution to protect the whole system). Threat identification is the first stage of the process after all. In this next phase, we classify those threats by giving them a priority express how urgent it is required that the threat be mitigated (reduced or eliminated). The final stage exclude vulnerabilities and introduce countermeasures to mitigate threats.

Conclusion

Finally, through the integration of STRIDE threat modeling framework with DREAD risk assessment you have a systematic approach to manage security in Electronic/ Smart Health Systems (EHS/SHS). Second, the integrated nature of this approach allows healthcare practitioners not only to locate potential threats but also to manage them in a comprehensive and preventive way with respect security and patient data privacy. STRIDE helps in a systematic identification of vulnerabilities and DREAD allow us to understand the risk related to each threat.

Through this collaborative approach, healthcare organizations can act pre-emptively to reduce risk exposure and lessen the likelihood of a security breach which invades patient data. This proactive approach enhances the overall security posture of EHS/SHS allowing zero data loss, and a resilient & secure implementation in real life healthcare scenarios. This is a conclusion demonstrating the need to mutually utilize these frameworks and further (ideally combined) reinforce the security and privacy of Smart Health Systems, thus resulting in increasingly reliable, trust-worthy healthcare environment.

5.1 Limitations

The validity of the work could be restricted to its limited scope i.e. our methodology might not be applicable to all the healthcare domains beyond Electronic or Smart Health Systems (EHS/SHS).

Resource Requirement: Implementing STRIDE and DREAD would need significant resource input as in the form of time, skills which may be a constraint for organizations that have less resources.

As the cybersecurity threat-scape is constantly changing and evolving, we must take this into consideration while modelling threats so that, if a discovered threat comes to adapt over time, which it simply will in most cases; the modeller can make appropriate modifications to their modelling process.

5.2 Future Work

Continued research in this field should focus on validation and generalization of the presented methodology for threat identification in EHS/SHS. A big opportunity to take an improvement is in the creation of a flexible and more scalable framework to meet modern security threats. Specialized threat models that address challenges in different healthcare settings should be developed with research efforts, rather than just focusing on EHS/SHS. Additionally, delving deeper on how prospective integration of new age technologies like AI/ML with respect to threat modelling may bring about fresh tactics for pre-emptive threats that can either be avoided or managed. Healthcare professionals and cybersecurity experts must continue to work closely together in order for future methods are developed that suit the increasingly nuanced requirements of the healthcare industry while providing sustainable solutions for patient data confidentiality and protecting the safety of health care operations. Finally, longitudinal studies should be conducted to assess the long-term success of this approach in healthcare settings and to identify processes that could be further improved through more precise threat identification.

Dedication

This work is dedicated to those who tirelessly strive for knowledge, innovation, and progress. To the dreamers who dare to challenge the status quo and envision a brighter future, and to the resilient souls who overcome obstacles with unwavering determination. May this endeavor inspire and contribute to the collective journey of human discovery. In honor of all those who believe in the power of curiosity, dedication, and the pursuit of excellence.

Acknowledgements

I would like to acknowledge and give my warmest thanks to my supervisor, Dr. Shariq Hussain, who made this work possible. His guidance and advice carried me through all the stages of writing my thesis. I would also like to thank my committee members for letting my defence be an enjoyable moment and for your brilliant comments and suggestions. I would also like to give special thanks to my parents and my family as a whole for their continuous support and understanding when undertaking my research and writing my thesis. Your prayer for me was what sustained me this far. Finally, I would like to thank God for letting me through all the difficulties. I have experienced your guidance day by day. You are the one who let me finish my degree. I will keep on trusting you for my future.

REFERENCES

Abughazaleh, Nada, R. Bin, and Mai. 2020. "Dos Attacks in IoT Systems and Proposed Solutions." International Journal of Computer Applications (British) 176 (33): 16–19.

Adeniyi, A. E., K. M. Abiodun, Joseph Bamidele Awotunde, Mukaila Olagunju, O. S. Ojo, N. P. Edet, and Applications. 2023. "Implementation of a Block Cipher Algorithm for Medical Information Security on Cloud Environment: Using Modified Advanced Encryption Standard Approach."

Multimedia Tools and Applications 82 (13): 20537–51.

Al-Muntaser, Bakil, Mohamad Afendee Mohamed, Ammar Yaseen Tuama, Imran Ahmad Rana, and Applications. 2023. "Cybersecurity Advances in SCADA Systems." International Journal of Advanced Computer Science and Applications 14 (8).

Albahri, Ahmed Shihab, Ali M. Duhaim, Mohammed A. Fadhel, Alhamzah Alnoor, Noor S. Baqer, Laith Alzubaidi, Osamah Shihab Albahri, et al. 2023. "A Systematic Review of Trustworthy and Explainable Artificial Intelligence in Healthcare: Assessment of Quality, Bias Risk, and Data Fusion." Expert Systems 96: 156–91.

Ali, Mansoor, Faisal Naeem, Muhammad Tariq, Georges Kaddoum, and IEEE Journal of Biomedical and Health Informatics. 2022. "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey." IEEE Journal of Biomedical and Health Informatics 27 (2): 778–89.

Almagrabi, Alaa Omran. 2023. "Challenges and Vulnerability Evaluation of Smart Cities in IoT Device Based on Cybersecurity Mechanism." Expert Systems 40 (4): e13113.

Almulihi, Ahmed H., Fawaz Alassery, Asif Irshad Khan, Sarita Shukla, Bineet Kumar Gupta, Rajeev Kumar, and Intelligent Automation and Soft Computing. 2022. "Analyzing the Implications of Healthcare Data Breaches through Computational Technique." Intelligent Automation and Soft Computing 32 (3).

Dwivedi, Ruby, Divya Mehrotra, and Shaleen Chandra. 2022. "Potential of Internet of Medical Things (IoMT) Applications in Building a Smart Healthcare System: A Systematic Review." Journal of Oral Biology and Craniofacial Research 12 (2): 302–18.

El-Bakkouri, N., and Tomader Mazri. 2020. "Security Threats in Smart Healthcare." The International Archives of the Photogrammetry, Remote Sensing, and Spatial Information Sciences 44: 209–14.

Gyamfi, Eric, and Anca Jurcut. 2022. "Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets." Sensors 22 (10): 3744.

Hasan, Mohammad Kamrul, Taher M. Ghazal, Rashid A. Saeed, Bishwajeet Pandey, Hardik Gohel, Ala'a Eshmawi, Sayed Abdel-Khalek, and Hula Mahmoud Alkhassawneh. 2022. "A Review on Security Threats, Vulnerabilities, and Counter Measures of 5G Enabled Internet-of-Medical-Things." IET Communications 16 (5): 421–32.

Hossain, Mohammad Naveed, Md. Mahedi Hassan, Raiyan Janik Monir, Md. Shaba Sayeed, Shaira Wajiha, and Tamkin Mahmud Tan. 2023. "Secure Internet of Things (IoT) Networks: Study the Challenges and Develop Solutions for Securing IoT Networks, Including Authentication, Access Control, and Data Protection." Asian Journal for Convergence in Technology 9 (2): 43–48.

Husnoo, Muhammad Akbar, Adnan Anwar, Nasser Hosseinzadeh, Shama Naz Islam, Abdun Naser Mahmood, and Robin Doss. 2023. "False Data Injection Threats in Active Distribution Systems: A Comprehensive Survey." Future Generation Computer Systems 140: 344–64.

Kumari, Ragni, Gaurav Dubey, Neha Dubey, and Nitesh Pradhan. 2023. "Artificial Intelligence Challenges, Principles, and Applications in Smart Healthcare Systems." In Machine Learning and Artificial Intelligence in Healthcare Systems, 1–24. CRC Press.

LaMalva, Grace, and Suzanna Schmeelk. 2020. "Mobsf: Mobile Health Care Android Applications through the Lens of Open Source Static Analysis." Paper presented at the 2020 IEEE MIT Undergraduate Research Technology Conference (URTC).

Lee, In. 2022. "Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach." Information 13 (9): 404.

Mahmoud, Hussam, Thomas Kirsch, Dan O'Neil, Shelby Anderson, and System Safety. 2023. "The Resilience of Health Care Systems Following Major Disruptive Events: Current Practice and a Path Forward." Reliability Engineering and System Safety 235: 109264.

Minopoulos, Georgios M., et al. "Exploitation of Emerging Technologies and Advanced Networks for a Smart Healthcare System." Applied Sciences 12, no. 12 (2022): 5859.

Parkavi, R., et al. "Data Breach in the Healthcare System: Enhancing Data Security." In Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies, 418–34. IGI Global, 2023.

Perez-Pozuelo, Ignacio, et al. "The Future of Sleep Health: A Data-Driven Revolution in Sleep Science and Medicine." NPJ Digital Medicine 3, no. 1 (2020): 42.

Rahaman, Md Shahidur, et al. "Access Control Design Practice and Solutions in Cloud-Native Architecture: A Systematic Mapping Study." Sensors 23, no. 7 (2023): 3413.

Thabit, Fursan, et al. "Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with Their Alleviating Techniques." Journal of Information and Computational Science 12, no. 10 (2020).

Thomas, Sade, and Lucien Ngalamou. "The Impact of Cybersecurity on Healthcare." Paper presented at the Future Technologies Conference (FTC) 2021, Volume 2, 2022.

Xu, Yixian, et al. "Exploring Patient Medication Adherence and Data Mining Methods in Clinical Big Data: A Contemporary Review." Journal of Evidence-Based Medicine 16, no. 3 (2023): 342–75.