

Threat Analysis for Healthcare IoT Devices

Safar Zabin Albaqami

Principal Supervisor: Dr Saeed Ur Rehman

28th August 2020

Submitted to the College of Science and Engineering in partial fulfilment of the requirements for the degree of Master of Science (Computer Science) at Flinders University – Adelaide, Australia.

Table of Contents

CHAPTER 1: INTRODUCTION 7

THE INTERNET OF THINGS AND THE INTERNET OF MEDICAL THINGS (IoMT) 7

HOW IoMT WORKS..... 8

Components of IoMT technology..... 8

THE NEED FOR PROTECTING PATIENT IoMT DATA 10

MOTIVATION 11

PROBLEM STATEMENT AND RESEARCH QUESTIONS..... 11

CONTRIBUTIONS 12

THESIS STRUCTURE 12

CHAPTER 2 : OVERVIEW OF INTERNET OF MEDICAL THINGS..... 13

INTRODUCTION 13

IoT MEDICAL DEVICES CONSTRAINTS..... 14

Resource Limitation 14

Mobility..... 15

Communication Heterogeneity..... 15

Data Heterogeneity 16

IoT MEDICAL DEVICES SECURITY 16

Data Security Challenges and Threats to Patient Data..... 16

Importance of Patient Data Security..... 17

SUMMARY 17

CHAPTER 3 : METHODOLOGY 18

INTRODUCTION 18

RESEARCH DESIGN 18

Quantitative Research Method..... 18

Qualitative Research Method 18

Mixed-Method 19

THE SIX STEPS OF RESEARCH DESIGN 19

Identify the Research Problem..... 19

Search criteria..... 20

Inclusion and Exclusion Criteria 20

Charting Data 21

Search Results..... 21

Research Gap..... 22

SUMMARY 22

CHAPTER 4 : LITERATURE REVIEW 23

INTRODUCTION 23

EVIDENCE 23

CONSEQUENCES OF USING UNSECURED IoMT DEVICES 25

CASE STUDIES..... 25

THE NEED FOR SECURITY SOLUTIONS 26

IoT ARCHITECTURE, SECURITY REQUIREMENTS, AND TECHNOLOGIES 26

IoT Perception Layer Cyber Threats 26

IoT Network Layer Cyber Threats..... 34

Application Layer Cyberthreats..... 45

SUMMARY	54
CHAPTER 5 : CHALLENGES AND SOLUTIONS	55
INTRODUCTION	55
THE THREE LAYERS OF IOT SYSTEMS	55
SECURITY THREATS AFFECTING PATIENT ELECTRONIC HEALTH RECORDS IN IOMT	56
<i>IoT Perception Layer Security Threats Analysis</i>	56
<i>IoT Network Layer Security Threats Analysis</i>	58
<i>IoT Application Layer Security Threats Analysis</i>	60
SUITABLE COUNTERMEASURES, CONTROLS, AND SOLUTIONS	63
<i>IoT Perception Layer Security Solutions Analysis</i>	63
<i>IoT Network Layer Security Solutions Analysis</i>	64
<i>IoT Application Layer Security Solutions Analysis</i>	65
CHALLENGES FACED WHEN SECURING HEALTH INFORMATION IN IOMT	69
SUMMARY	77
CHAPTER 6 : DISCUSSION	78
CONCLUSION	78
FUTURE WORK	80
REFERENCES.....	81

List of Figures

FIGURE 1: HOW IOMT WORKS IN A HOSPITAL SETUP [3]	8
FIGURE 2:DATA FLOW DIAGRAM	13
FIGURE 3: DISCUSSION CHAPTER STRUCTURE	55
FIGURE 4: IOT ARCHITECTURE	56
FIGURE 5: SUMMARY OF IOT PERCEPTION LAYER SECURITY ATTACKS	58
FIGURE 6: SUMMARY OF IOT NETWORK LAYER SECURITY THREATS	60
FIGURE 7: SUMMARY OF IOT APPLICATION LAYER SECURITY THREATS	62
FIGURE 8: SUMMARY OF POPULAR SECURITY SOLUTIONS FOR IOMT	67
FIGURE 9: ENCRYPTION MECHANISMS PROPOSED FOR SECURING IOMT SYSTEMS AND HEALTHCARE DATA.....	67
FIGURE 10: ACCESS CONTROL MECHANISMS USED TO ENSURE IOMT SECURITY	68

List of Tables

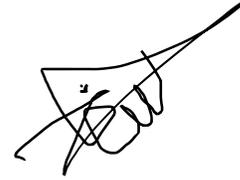
TABLE 1: COMPARISON BETWEEN IOT AND IOMT	7
TABLE 2: SEARCH RESULT STATISTICS	21
TABLE 3: IOT PERCEPTION LAYER CYBERTHREATS	29
TABLE 4: IOT NETWORK LAYER CYBERTHREATS	37
TABLE 5: IOT APPLICATION LAYER CYBERTHREATS	49
TABLE 6: SUMMARY OF THREATS/ATTACKS IN THE PERCEPTION LAYER	57
TABLE 7: SUMMARY OF THREATS/ATTACKS IN THE NETWORK LAYER	59
TABLE 8: SUMMARY OF THREATS/ATTACKS IN THE IOT APPLICATION LAYER	61
TABLE 9: SUMMARY OF SOLUTIONS TO IOT PERCEPTION LAYER SECURITY THREATS.....	63
TABLE 10: SUMMARY OF SOLUTIONS TO THE IOT NETWORK LAYER SECURITY THREATS.....	64
TABLE 11: SUMMARY OF SOLUTIONS TO THE IOT APPLICATION LAYER SECURITY THREATS.....	65
TABLE 12: CHALLENGES FACED WHEN SECURING IOMT AND HEALTHCARE INFORMATION	76

Abstract

The monitoring devices of the healthcare system are components of the Internet of Medical Things and are connected to cloud services, servers, clients and databases. These devices monitor the patient's status remotely by recording and transferring particular measurements to patient record management systems. Patient data appear to be very sensitive as it is used and interpreted as the health record of the patient. There are security and privacy requirements for data generated by IoT technology in healthcare, and there are multiples studies that conduct thorough threat analysis in order to reduce IoT devices attacks. It is important to provide the results of current studies more accessible to the healthcare manager. Therefore, it is required to identify, evaluate and categorise the summaries of each study over IoT security issues, solutions and challenges. This study employed a systematic review method to provide in-depth information about IoT threats analysis. Our finding provided the security threats affecting patient electronic health records collected and processed through medical wearables and sensor-based IoT devices and cloud information management such as DDoS, man-in the-middle attack, eavesdropping, physical data tampering, privacy attacks, false data injection, and brute force attacks, hardware misconfiguration, data exfiltration, tampering, email spoofing, social engineering (phishing), security misconfiguration, exhaustive search attacks, sensor hijacking, cloning, flooding attacks, on-off attacks, and worm-based cyber threats. Additionally, the study identified suitable countermeasures, controls, and solutions that healthcare facilities can implement to protect patient health data collected through IoMT and stored in a cloud environment such as data anonymization, privacy-preserving data aggregation scheme, proxy re-encryption, cryptography, user access control, authorization, blockchain, anti-DDoS and hybrid privacy preservations systems. Finally, the study outlined the challenges healthcare institutions face when securing patient health records in a cloud environment and medical IoT devices such as difficulties in securing massive data collected by IoMT, hackers introducing frequent and sophisticated threats that bypass implemented security controls, security teams facing difficulties in security devices located in an extensive area network. Besides, healthcare service providers lack concrete system development knowledge for some of the recommended solutions, such as blockchain technology. Ultimately, this study is crucial for the healthcare sector, medical device manufacturer, clinicians, authorities, and patients seeking to prevent malicious actors from infiltrating IoMT devices and information.

Declaration

I certify that this work does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university, and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.



Safar Zabin Albaqami

28th Aug 2020

Acknowledgment

I would like to thank God Almighty for giving me the ability, opportunity, knowledge and strength to complete this research project satisfactorily. This achievement would not have been possible without his blessings.

I would like to thank my supervisor, Dr Saeed Ur Rehman, for his support during my first research project. His expertise and knowledge motivated me and gave me the confidence to write a research thesis for the first time. I would like to also express my sincere and greatest gratitude to my thesis coordinator, Dr Anna Shillabeer, for her continuous support of my research.

I would like to acknowledge the Ministry of Science, Saudi Arabia, for funding through that supported my study. In addition, I would like to thank the Flinders University library for providing the resources I have needed to complete my research project.

I must express my very profound gratitude to my parents Mrs Ghalbaa Albaqami and Mr Zabin Albaqami and to my wife Mrs Ghzwh Albaqami for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. I am grateful to my sisters Mrs Muneerah Albaqami, Mrs Salha Albaqami and my brothers Mr Saad Albaqami, Mr Muslih Albaqami, for always being there for me as close friends. Thank you.

Chapter 1: Introduction

The Internet of Things and the Internet of Medical Things (IoMT)

There is a stark difference between the Internet of Things (IoT) and the Internet of Medical Things (IoMT). The Internet of Things is the collection of billions of interconnected devices connected to the Internet to assimilate and share data. The IoT is composed of numerous devices that mainly consists of sensors in refrigerators, cars, smartphones, aeroplanes, thermostats, and so on. The IoT allows the devices to connect over the web such that their endpoint levels are nearly autonomous and sufficiently intelligent [1]. The endpoints enable them to intelligently analyse and process data without necessitating the manual intervention of humans. The IoT is broad, given that it comprises all the things which can connect to the Internet.

On the other hand, the Internet of Medical Things consists of only the devices connected through the Internet that are used to provide improved and optimized medical care. They only benefit and impact individuals seeking specialized care, which requires round the clock monitoring [2]. Also, there is a big difference in the technologies embedded in IoT and IoMT. The IoT is designed to perform any function within their respective industry, whereas the IoMT is intended to facilitate health care provision. These differences have been illustrated in table 1.

Table 1: Comparison between IoT and IoMT

	IoT	IoMT
Use Cases	IoT covers a variety of new technology solutions used in many industries, including construction, industrial environments, and at home	IoMT features connected devices used in the medical and healthcare sectors
Design	IoT is consumer-focused and is designed to provide maximum usability and convenience.	IoMT is designed to provide reliability, accuracy, and enhanced security
Target customers	A majority of IoT branded devices target average customers. They do not require additional skills to operate	IoMT requires additional knowledge to interpret the device's operations and data
Regulations	General application IoT is less regulated	IoMT faces strict security protocols and HIPAA compliance

How IoMT Works

Figure 1 [3] below is an example of the usage of IoMT in a hospital setup.

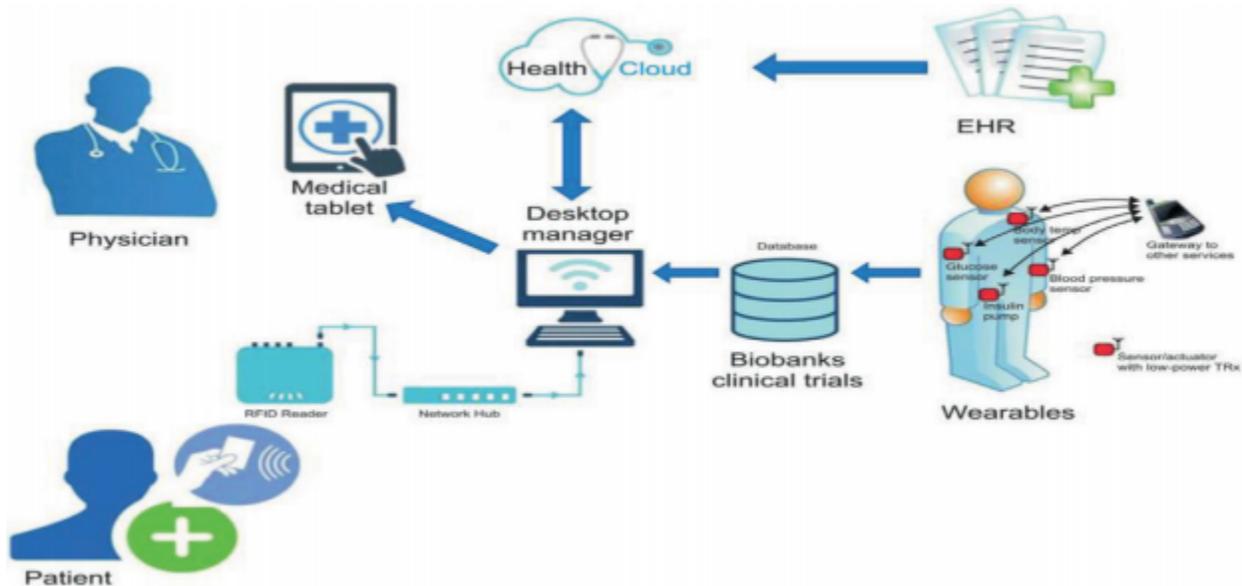


Figure 1: How IoMT works in a hospital setup [3]

As illustrated in figure 1, a patient has different wearables that collect and record vital health data and stores it in a cloud. The scanning of a patient's ID card links automatically to the secure cloud housing sensitive electronic health records, prescription and medical history, lab results, and patient vitals. The data provides physicians with numerous benefits, including monitoring patient health, fitness programs, elderly care, and chronic diseases remotely. Additionally, healthcare practitioners use ubiquitous sensors and the Internet to control and share patient health data between objects, humans to objects, and humans to humans. Various medical equipment, imaging, and diagnostic devices, and sensors are a core part of the IoMT ecosystem. The data flow process is susceptible to multiple threats since attackers can target the numerous entry points, including patient wearables and the cloud.

Components of IoMT technology

a) Artificial intelligence

Artificial intelligence in healthcare is an essential component of the Internet of Medical Things. Incorporating artificial intelligence in healthcare provides avenues for physicians to discover patterns from learning patient activities in connected devices for healthcare monitoring. Besides, artificial intelligence finds patterns through analysis of patient transactions, which accords healthcare providers the ability to provide preventive care [4]. Due to artificial intelligence advancements in healthcare, preventive health care models based on artificial intelligence have been developed. Moreover, artificial intelligence in health

care is advantageous since it creates a system whereby the health care system itself can continuously learn. Continuous learning enables health care providers to provide care based on patients' past treatments, medical records, and the evolution of various treatment methods [5]. Artificial intelligence allows the digitization and automation of the knowledge mined from different medical sources, including connected devices, medical staff, nurses, and doctors. Combining all the acquired knowledge facilitates the provision of optimized patient care.

b) Healthcare Value Streams Digitization

Patient end-to-end value streams require to be captured and be digitized. Optimizations and efficiency in most health care facilities are improving their leverage on dynamic case management and intelligent business process management. Healthcare institutions often undertake repetitive work and activities, such as entering and storing patient data. Such actions are being augmented or automated through the use of artificial intelligence. Other categories in which value streams digitization has greatly improved are cognitive work, and knowledge of both nurses and doctors and artificial intelligence assisted work for medical workers and other relevant medical categories [6].

There are numerous applications of all the three components, which constitute of Internet of Medical things with multiple IoT devices. Wellness tracking enables physicians to remotely monitor and keep track of a patient's fitness and health. Wellness tracking is used in monitoring temperature, blood pressure, and heartbeat rates. IoMT devices used for such applications include sensor devices, smartwatches, and Fitbit. They also apply to home healthcare provisioning for the elderly. Seniors typically prefer living in their homes as compared to hospitals or rehab centres. Telecare and connected and monitoring devices are used to monitor older adults in their homes. Also, the aforementioned IoMT categories have led to the development of intelligent hospitals. Connectivity of IoMT devices has numerous valuable and pragmatic applications that lead to the overall improvement in the running and operation of smart hospitals. Other critical applications of IoMT categories include but are not limited to digital and prescriptive maintenance of hospital and medical equipment.

c) IoT Medical Devices and Connected Wellness

The Internet of Things Connected Wellness and Medical Devices IoMT component focuses on digital health technologies with more focus on the consumer. Digital health technologies are rapidly growing due to innovative solutions continuously developed for treating, monitoring, and diagnosing illnesses. Moreover, to provide optimized and quality healthcare services, the Internet of Medical Things and devices are increasingly becoming connected and intelligent. They are also being developed to be more robust. The importance of developing and advancing IoMT and connecting medical devices is to

incorporate the use of information technology in providing excellent medical services [7]. The opportunities of information technology in medical devices include improving patient data storage, management, and retrieval, remote health care provisions, and monitoring, and providing advanced treatments to patients with adverse medical conditions.

The Need for Protecting Patient IoMT Data

Protecting patient IoMT data is vital since it is exposed to multiple security threats. For instance, IoMT relies on network connectivity to function correctly. Attacks on a hospital network is an attack on the functionality of IoMT devices. There are many methods in which cybercriminals can attack the network connecting IoMT devices and technologies. Some of the most common ways to conduct attacks are traffic analysis, RFID spoofing, RFID cloning, sinkhole attack, and man in the middle attack. Irrespective of the method used, hackers can quickly gain control of data IoMT data communicated through a compromised network. Unauthorized access and control may cause patients to miss essential appointments with their physicians, lead to the wrong prescription of medication, or even lead to health care providers being able to provide optimized care to patients. In other cases, network attacks may lead to monitoring tools that relay the wrong information regarding a patient's health, consequently causing physicians to provide incorrect medical advice, which may further propagate the patient's health. One principal aim of the Internet of Medical Things is to enable doctors to monitor patients' health remotely and offer medical advice based on the observation of the patient data. Interfering with the network in which such devices are connected to leads to wrong medical information and treatment being administered [8].

Also, some of the IoMT devices may develop connectivity and network glitches, which may go unnoticed. The glitches may cause interference and vulnerabilities in the movement and transference of confidential patient data in the data migration process [9]. Also, network and connectivity issues may prompt the transfer and migration of data to unauthorized individuals connected on the same network. As a result, the problems pose severe issues if rogue IT personnel, hackers, or even unlicensed vendors place standalone IoT devices on the system and hence capture valuable data. In most cases, connectivity and network glitches may prevent healthcare IT personnel from noticing new standalone devices added to the network. Again, unnoticed devices pose immeasurable security risks since unauthorized individuals who operate on a system undetected may perform any illegal actions. These may compromise the transparency, integrity, and confidentiality of the health data of the affected health care provider [10].

Motivation

IoMT technologies store highly sensitive information during care provisioning. Therefore, the security and privacy of such data are paramount to protect the information from unauthorized access, breaches, and compromise of its availability, integrity, and confidentiality. Hence, four factors motivated the analysis of threats affecting healthcare IoMT devices as they relate to patient data privacy and security. They are:

- a. Privacy Acts and legislation: Various privacy Acts and legislation, such as the Office of the Australian Information Commissioner (OAIC) regulations and the National Health and Medical Research Council (NHMRC) guidelines, and the 13 Australian Privacy Principles (APPs) of the Privacy Act 1988, obligate health providers to implement safeguards and practices to ensure the privacy and security data. Understanding security threats to healthcare IoT is crucial to informing the necessary controls to comply with the regulation requirements.
- b. IoT security threats affect physical security: Hackers can compromise unsecured IoMT devices to breach the physical safety of a health facility. Compromised physical security can allow cyber adversaries to gain unauthorized access to other essential assets, including networks, information, and other IT infrastructure.
- c. Gain more insight into patient data security: Analysing security threats to healthcare IoT will provide a detailed overview of the various challenges that security teams face when protecting patient data within cloud and IoT environments. The analysis will thus inform suitable solutions to address the problems.
- d. Understand security threats to patient data: IoMT technologies play a vital role in healthcare treatment and provisioning, but also expand the threat surface. A threat analysis of healthcare IoMT can provide a better understanding of such threats and appropriate controls for mitigating them.

Problem Statement and Research Questions

IoMT technologies have become a convenient means of delivering quality care remotely. Every year, new IoMT technologies emerge, bringing along new security threats and risks. On the other hand, patient data contains highly sensitive information. Compromising the data's integrity, availability, and confidentiality may severely affect a patient. It can lead to death, delayed healthcare provisioning, wrong prescriptions, and medication, or prevent patients from accessing critical care services. Security threats in IoMT are pervasive, and this research attempts to address the following three questions:

- a. What are the security threats affecting patient electronic health records collected and processed through medical wearables and sensor-based IoT devices, and cloud information management?
- b. What are the suitable countermeasures, controls, and solutions that healthcare facilities can implement to protect patient health data collected through IoMT, such as wearables and sensor devices, and stored in a cloud environment?
- c. What challenges do healthcare institutions face when securing patient health records in a cloud environment and medical IoT devices?

Contributions

The research makes the following three essential contributions to the IoMT industry:

- a. Identifies security threats to patient electronic health records, in healthcare IoT technologies
- b. Describes the security solution for ensuring patient data security and privacy
- c. Highlights the IoT security challenges that reported in the literature

Thesis Structure

The rest of the chapters in the thesis are as follows; chapter two provides an overview of IoMT that collects patient information and parameters and describes the data flow from collection to storage in various stages. Also, chapter two explores the IoMT device constraints, including restricted resources communication and data heterogeneity, and the mobility of IoT embedded in humans. Moreover, chapter two discusses security in IoMT by focusing on data security challenges, possible solutions for alleviating the security risks, and the essence of securing patient information collected through healthcare IoT devices. Chapter three discusses the research methodology by systematically reviewing papers, journal articles, and publications on IoT patient data selected through processes, such as data extraction and querying computer science databases. The chosen papers are used to develop the literature review on various IoMT security topics in chapter four, while chapter five discusses the findings. Chapter six concludes by reviewing the identified threats and recommended solutions.

Chapter 2 : Overview of Internet of Medical Things

Introduction

IoMT technologies have enhanced the delivery of quality healthcare but have also led to an increase in threats and risks associated with the security of IoT devices. Service delivery and patient satisfaction can be considerably affected in the event of a cybersecurity emergency. Any situation that compromises the integrity, confidentiality and availability of data has the potential to result in adverse consequences such as death, prescription, and medical errors, or delayed healthcare provision. Today, collecting and managing patient health information utilizes various devices to facilitate effective service delivery and decision making. Examples of such devices include medication administration equipment, assistive technology, monitors, telehealth devices, and infant care, among others. In a healthcare setting, these devices form part of the data flow components, as illustrated in Figure 2:

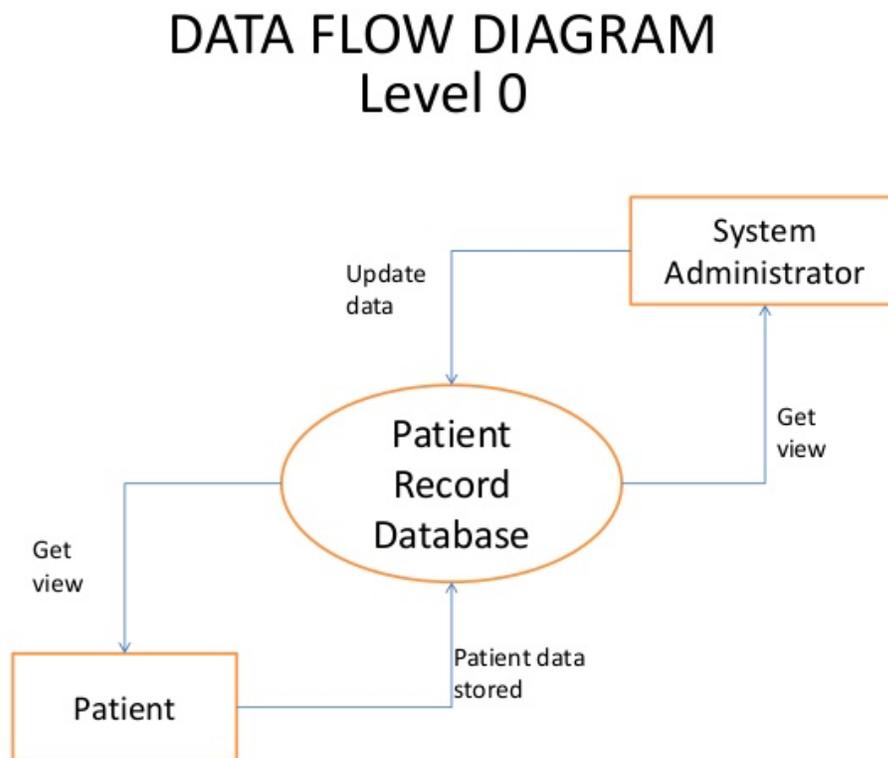


Figure 2:Data flow diagram

Smart devices collect and store data in the cloud, which links to other sensitive health data, including patient records, vitals, laboratory results, and medical history. Data in transit form a fundamental stage in the data flow as information is continually collected and shared with practitioners and physicians. This chapter explains the Internet of medical things, with a focus on device constraints

and security. The constraints that are described in detail include resource limitation, mobility, communication, and data heterogeneity. This study also highlights threats to confidentiality, integrity, and availability for these IoT medical devices. This overview of IoMT constraints and risks will help the reader understand subsequent chapters.

IoT Medical Devices Constraints

The growth of internet technology has brought about several vulnerabilities in the context of cyber insecurity. The Internet of Things and associated networks remain vulnerable to cyber-attacks and system failures. The exploitation of these vulnerabilities allows attackers to manipulate, change, alter, or destroy the system, which can affect the delivery of healthcare services and compromise medical outcomes. Medical IoT devices remain vulnerable to attack because the increase in these instruments makes it difficult for IT technicians to employ unified approaches in endpoint management [11]. The adoption of IoT devices in the healthcare setting changed service delivery by reducing costs and improving service delivery. Still, the risks and threats associated with cybersecurity vulnerabilities may introduce unquantifiable costs to the industry. Below are some of the security challenges of IoMT.

Resource Limitation

One of the significant issues associated with the use of IoT devices in the medical setting is that they are severely limited. A variety of factors contribute to this limitation, including the fact that they are incredibly resource-constrained [12]. For example, some devices are known to have modest hardware that uses less efficient batteries. Battery life is a significant limitation that increases the risks associated with IoT medical devices. Most of these devices use non-rechargeable batteries that do not last for more than a few years. Furthermore, when the user undertakes one expensive processing, it takes away several weeks of the battery's life. This limitation makes it difficult for IoMT devices to be reliable when implementing standard cryptographic security controls.

Nothing can be more frustrating than for a patient to find out that their heart monitoring smartwatch or pressure monitor is low on charge. It can delay the detection of vital conditions and limit access to critical interventions. A majority of the wearables have batteries that do not last for long and require almost daily charging, an aspect that reduces their effectiveness. Battery life does not develop at the same rate as other medical IoT technologies, which limits the usability of devices.

Users also face a limitation when attempting to integrate wearables and sensors into their daily lives due to a problem with the charging mechanism. As the IoMT devices continue to become smaller and more complex, charging mechanisms are also evolving, making it difficult for users to operate them effectively [13]. It is a limitation that elderly patients encounter difficulties daily as they attempt to run

the devices themselves. For them, they may need external assistance with their hearing aids or heart monitors, further complicating matters for patients and their primary caregivers.

Mobility

Mobility is a constraint for patient data security because IoMT devices and their networks are deployed on a large scale. They deal with human-related information, and as such, the mobility of patients plays a crucial role in determining the effectiveness of the devices [14]. Communication between the devices and the network system is through gateways that act as connection points. For patients who are confined to hospitals or homes, their location and reduced mobility ensure the gateways play a critical role. As such, the stationary nature of the patients and the devices attached to them makes it easier for them to work as they will not be constrained. However, in cases where the mobility of the patient is not manageable, the devices will be resource-constrained in terms of energy consumption. As already explained, such devices are already limited in terms of battery usage. In situations where there is increased mobility, charging the devices becomes a challenge.

With increased mobility, comes other constraints as well. The devices will be constrained in terms of communication bandwidth and memory usage. In such situations, it is not easy to provide the necessary security context related to the medical sensors. Without the problem of mobility, smart gateways operate by eliminating the need to authorize and authenticate the healthcare providers⁸. This makes it challenging to block any malicious activity, hence increasing the security vulnerability of these devices. Increased patient and device mobility do not guarantee patients the assurance that the monitoring of their health is not interrupted. For medical practitioners, this is cause for worry as they cannot collect critical data about the patient's vital signs.

Communication Heterogeneity

There is a growing ambiguity associated with IoT devices, especially in a medical setting. In an age where numerous smart devices can be connected to a network system, it is mandatory to maintain a standard lightweight communication stack to provide solutions to connectivity and interoperability issues². Communication heterogeneity in the use of IoT devices in a healthcare setting is attributed to the presence of multiple wireless technologies connected to the cloud. This includes the numerous sensors and other devices used on patients. It is a problem that is significant, especially when it comes to designing these connected IoMT. As a result, standardization becomes very difficult to achieve, primarily because there is no single technology that can be relied upon to provide solutions to all requirements of the IoT network. Ultimately, this communication heterogeneity compromises several aspects of the devices, including service quality, bandwidth, operational costs, power consumption, and latency among others².

Data Heterogeneity

For effectiveness and reliability to be sustained, it is crucial for information collected and shared by these devices to observe the quality of service standards. However, this is not always the case, as there is a deficiency of data standards for smart devices in a healthcare setting [15]. There is an issue of interoperability due to the problem of data heterogeneity attributed to the diversity of IoT devices. Different devices have different designs because they come from distinct vendors. As a result, they have different methods of syntactic and semantic interoperability. For this reason, there is always the risk of syntax and semantic errors. In essence, it is difficult to add a new device to the network without syntactic conflicts and semantic ambiguity.

IoT Medical Devices Security

Data Security Challenges and Threats to Patient Data

Numerous data security challenges continue to impact reliance on IoT devices in the healthcare setting. One of these issues is the integrity of the devices. In a medical situation, the devices should offer accurate, precise, and objective results. Indeed, the integrity of devices such as heart monitors and sensors are paramount for decision making on diagnosis, treatment, prevention, and monitoring. Device security is essential as it impacts the safety and effectiveness of the devices used. The data generated by the apparatus is what forms the basis of pathological processes. Drug infusion pumps and pacemakers are examples of the tools that are required to provide reliable and accurate data. Markedly, the integrity of devices subsequently affects the integrity of data collected. The health sector is predominantly reliant on information. In the case of wrong or inaccurate information, it will affect subsequent processes, including diagnosis and treatment plans recommended. Ultimately, this will result in adverse medical outcomes, including death. IoMT devices must provide reliable information, but this is not always the case as such systems remain vulnerable to loss of data integrity.

Confidentiality is another data security problem associated with smart devices. It is defined as the state of ensuring and protecting privacy. Indeed, there is a correlation between confidentiality and the lack of privacy. Smart medical devices collect a wide range of patient information, including sensitive data such as personal and family details. Since the devices are connected to network systems, there is always a threat of hacking and other forms of cyber-attacks. This problem is not restricted to the health sector only, as privacy and confidentiality remain issues of concern for individuals, organizations, and governments alike [16]. The loss of data privacy and confidentiality to unauthorized users compromises security as the information can be used for malicious purposes. It is the reason why data protection is a core compliance issue for many organizations that deal with sensitive information, including those in the

health sector. As the cyber technology evolves, so do the methods that cybercriminals used to hack, or gain access into networks [17]. As such, the facility needs to utilize these devices to ensure consistent monitoring and evaluation to identify gaps for improvements in network and system security.

Availability is another crucial data security problem for users of IoMT devices. It is one of the core requirements for a reliable network system, denoting the accessibility of information to authorized users. Availability is a fundamental attribute of data networks that provides the assurance that the system and information contained on it are assessable to authorized personnel. In the health care setting, medical practitioners and physicians need the guarantee that they can access patient information at any time. It is an attribute that holds great value, similar to integrity and confidentiality. Smart medical devices face the risk of compromised availability in case of cyber-attacks that cripple, disable, erase, or destroy sensitive information and systems. In such a case, the devices are no longer dependable and can result in unforeseen consequences. Addressing these threats demands the implementation of the best solutions that protect patient data. These solutions must ensure robust protection for the network, system information, and any other cyber components. This will require the development of effective policies to reduce vulnerabilities, compliance with data security protocols, and training users on the appropriate use of the networks and systems to avoid internal threats.

Importance of Patient Data Security

The importance of maintaining the security of patient data cannot be underestimated, especially in terms of the contribution to medical outcomes. Broadly, patient data security guarantees the protection of sensitive information, helping to maintain confidentiality and privacy. Moreover, secure devices and systems provide accurate and reliable information free from external manipulation by unauthorized or malicious users. As such, secure networks facilitate decision making concerning diagnosis, treatment plans, prevention strategies, and follow-up measures. Generally, patient data security is essential in guaranteeing positive medical outcomes and saving lives.

Summary

This chapter has explored the use of IoMT devices in the medical setting. Specifically, the chapter analyses the constraints associated with the use of smart devices. Some of the limitations explained include resource limitations, mobility, as well as data and communication heterogeneity. The chapter has also explained the concept of IoT medical device security by discussing the data challenges and threats to patient information, recommending possible solutions, and revealing the importance of patient data security collected by IoT devices.

Chapter 3 : Methodology

Introduction

The chapter aims to describe the research methodology and design for addressing the research questions outlined in Chapter One. This method illustrates the plan for collecting data for addressing the research questions. There are three types of data to collect:

- i. Quantitative data (numbers),
- ii. Qualitative data (words), and
- iii. A mix of statistical data and descriptive data [18]

Research Design

There are three types of research methodologies (1) quantitative method, (2) qualitative method, and (3) mix method. Quantitative research is the process of making predictions, finding patterns, generalising results from a sample to a wider population or testing the relationships from analysing numerical collected data systematically [19]. According to Sukamolson et al. [20] "*quantitative research is the numerical representation and manipulation of observations to describe and explain the phenomena that those observations reflect*". This methodology is used in most of the natural and social sciences [20]. In contrast, qualitative research is a systematic approach that looks for building discussions from non-numerical data to interpret their meaning that helps the researcher to understand the science phenomenon [21]. According to Fossey et al. [22] "*qualitative research is a broad umbrella term for research methodologies that describe and explain persons' experiences, behaviours, interactions and social contexts without the use of statistical procedures or quantification*". This methodology is commonly used by social science researchers [22].

Quantitative Research Method

This type of method generates data that is numerical or can be converted into statistics. Moreover, quantitative methods usually use statistical or mathematical methods for the analysis of collected data. Surveys, questionnaires, and experiments are standard tools for collecting quantitative data [23].

Qualitative Research Method

The data produced by a qualitative method is in the form of text. This method provides a deeper understanding of how the researcher grabs and manage their research tasks in particular settings.

Reviews, observations, interviews, and discussions are universal instruments for collecting qualitative data [24].

Mixed-Method

The mixed research method data can be in both forms of numbers and text. This method is useful when the researcher needs to combine the elements of qualitative and quantitative methods. Usually, the results of one method (qualitative or quantitative) can be extended by the result of the other one. The data collection tools of this method can be the combination of qualitative and quantitative data collection instruments such as interviews and questionnaires [25].

The Six Steps of Research Design

This study will use a qualitative research method, among the three types of methods described above. A systematic review is carried out to extract and analyse the related concepts to patient threat analysis in the IoMT ecosystem. This method extracts qualitative data from the articles of selected scientific databases to evaluate threats for patient data, summaries the threat's solutions, and report the gaps/challenges. The systematic review defined [26] as "a means of evaluating and interpreting available research relevant to a particular research question, topic area, or phenomenon of interest". This type of review identifies the most relevant evidence, which answers the research questions [26]. It is important to have a plan for developing a systematic review, that clarifies all the involved review steps in a structured manner. The Daudt et al. [27] framework is adopted for reviewing patient threat analysis in IoMT ecosystem as methodology and material selection. This framework has six steps that facilitate this study's review plan, namely: (1) Identify the research problem, (2) Search criteria, (3) Inclusion and exclusion criteria, (4) Charting data, (5) Search results and (6) Research Gap. The research design based on these six steps systematic review methodology is detailed in the next sections.

Identify the Research Problem

Daudt et al. [27] framework suggest identifying the research questions as the first step of the framework. Our research aims to analyse the patient data threats where the data is collected from IoT devices and sensors. Moreover, the proposed countermeasures that prevent the damage or help to recover from attacks are reviewed. In addition, this study also examines the challenges that are existed to protect patient data in medical sensor-based devices. Our research questions are identified below:

1. What are the threats to patient record data?
2. What are the countermeasures (or solutions) available for protecting patient record data?
3. What are the challenges to protect patient record data?

The focus of the first question is on providing the threats provided by other studies where the IoT devices are used to collect the data. Our study addresses question 1 with categorising the threats based on the IoT architecture and how data flows from patient to data storage. Moreover, the list of countermeasures provided for the threats (mentioned above) addresses the second question. To address the last question, we summarise the open issues identified by studies that have reviewed.

Search criteria

Daudt et al. [27] second step suggests to identify relevant studies and to do a comprehensive review, which helps to achieve the aim of the systematic review. This study adopted a strategy for choosing the most relevant studies. The studies are identified by using the advanced search option of electronic databases such as IEEE Xplore, Science Direct, Elsevier and bibliographies within references. For searching the articles, the following terms are used with an AND operator: patient data protection, patient IoT data privacy, data security IoT devices, data security medical IoT devices, data security IoT cloud computing.

Inclusion and Exclusion Criteria

The third step of Daudt et al. [27] is about filtering the identified articles using the inclusion and exclusion criteria. The following criteria are applied to the relevant literature:

i) Inclusion criteria

- (1) Research published during the interval 2010 to 2020
- (2) The research focused on threats for patient data in IoMT ecosystem
- (3) The research provided a solution for the threats
- (4) The research provided the challenges for protecting patient data against the threats
- (5) Conference proceedings review and review papers
- (6) Peer-reviewed papers
- (7) Full papers

ii) Exclusion criteria

- (1) Studies published before 2010 were excluded as the IoT enabled by grouped of companies, and they promoted the use of IP in the network of smart objects in 2008, and it also attracted more interest when the IPv6 launched at 2011 [28]. There might be some studies from 2008 to 2010 that they may already be covered through the references of studies after 2010. Further, the research on IoT and its use in health sector geared up after 2010. Therefore, we are only considering paper after 2010.
- (2) The non-English articles are excluded

- (3) The theoretical articles that discussed the algorithmic and mathematical methods to implement a security algorithm (encryption / decryption) are excluded
- (4) Studies that do not have the technical material for our charting data (next step) such as the threats names or their countermeasure (data useful for chart preparation) are excluded
- (5) Duplicates are also excluded from the relevant articles

Charting Data

Charting data is the fourth step of daudt's framework. A chart can be used to extract the following data from the selected relevant studies:

- i) Technical material
 - (1) Threat / Attack names
 - (2) Data flow detail
 - (3) Security issues
 - (4) Solution (methods)/ challenge (issues)
- ii) Article details

Search Results

The fifth step is to summaries and reports the results in the form of a table or chart. This step highlights the total number of identified relevant articles and also the exclusion and inclusion numbers.

The result of search has been illustrated in table 2.

Table 2: Search result statistics

Criteria: Terms	# of Results	# of Results 2010-2020	# of Result Full Articles	# of Result Related Content
Patient data protection	73	50	49	7
Patient IoT data privacy	10	9	7	2
Data security IoT devices	325	324	299	23
Data security medical IoT devices	44	44	40	7
Data security IoT cloud computing	269	269	247	7
Total relevant studies searched:	721			
Total of exclusion criteria 1:		696		
Total of exclusion criteria 2:			642	
Total of exclusion criteria 3: related title and abstract of the searched articles (excluding duplications):				46

This thesis reviewed another 39 articles to provide sufficient information for introduction, background (IoMT standards, regulations and definitions), and overview of Internet of Medical Things.

Research Gap

In the last step, this study identifies the research gaps and report them under the Future Work section of this thesis.

Summary

This chapter outlined the research plan for this study. We are conducting a systematic review to address the research questions (discussed in Chapter 1). The next chapter provides the secondary review of the literature and categorises the information based on the IoT architecture layers.

Chapter 4 : Literature Review

Introduction

Contemporary healthcare settings are increasingly using IoMT technologies to enhance the quality of healthcare. These technologies have become especially important in providing quality health services remotely. Nonetheless, despite the distinct advantages associated with the use of IoT devices in delivering medical care, concerns remain over the security risks that threaten the effectiveness and efficiency of IoMT technologies. The problem is that these risks and threats pose a significant challenge to sensitive patient data, as they compromise the integrity, confidentiality, and availability aspects. Such threats can adversely affect patients as well as the facilities and practitioners delivering remote healthcare. The subject is essential because cyber-security threats to IoMT technologies can result in risky medical outcomes, delayed interventions, inaccurate prescriptions, and subsequent medication, compromised access to critical services, and possible death of patients.

This chapter adds to the analysis provided in the previous chapters by providing more description of the problem and discussing the urgent need for security solutions. The chapter analyses data threats based on IoT secure architecture [29-31] that has three layers such as perception, network, and application layers. This report describes each layer of the IoT architecture, as well as the security requirements. The data provided in this chapter will help to answer the research questions identified in the first chapter by developing an in-depth analysis of previous studies on precise security topics in the context of IoMT security. The next chapter will discuss the research questions based on this review chapter.

Evidence

The world has witnessed considerable progress in terms of the adoption and use of IoT medical devices in the healthcare setting. According to recent studies, researchers report that the use of IoMT saves the health industry about \$300 million annually as a result of remote service provision and improved medical outcomes that reduce readmissions and healthcare costs [32]. Nonetheless, this progress comes with new security challenges as the systems are more challenging to monitor and protect. Today, more than 60% of medical devices are vulnerable to different types of cyber threats [33]. There is a growing need to address these risks and find lasting security solutions even as analysts expect the IoMT sector to grow in value from about \$15 billion to more than \$50 billion in the next two years [33]. It is essential for all stakeholders in the healthcare system, including practitioners, patients, and IT experts, to gain insight

into the vulnerabilities of these IoT devices and develop practical solutions to ensure protection is enhanced.

It is not easy to determine how exactly IoMT devices are vulnerable, but the healthcare industry is one of the most targeted by cybercriminals. According to [34], more than 30% of all patient data breaches in the US happen in hospitals. It is an alarming statistic given the fact that there are an estimated 120 million medical devices connected to IoT in the country, all of which remain at risk of cybersecurity incidents [35]. The BlueKeep cyberattack is one of the reminders of the security issues that IoMT devices face. Security teams fear a recurrence of the WannaCry attack, where EternalBlue was deployed as a worm, resulting in adverse implications for tens of thousands of medical facilities and devices in Scotland and the UK [36]. The security threat facing IoMT equipment is real, and some hospitals in the US have resulted in turning away patients after hackers compromise their systems. Evidently, such a security incident affects healthcare service delivery and can result in tragic consequences for affected patients.

Security experts have repeatedly warned about the vulnerability of these devices, but most hospital systems remain susceptible to a cyber-attack. The situation is critical for Windows devices since almost 25% of the IT systems found in typical hospitals are prone to worms such as BlueKeep. One reason for this vulnerability is the lack of proper patching. Moreover, cybersecurity teams associate the risks associated with IoMT devices with human error. Recent findings indicate that internal misconduct caused more than 55% of all security incidents in the healthcare sector [37]. It means that most of the harm caused by cybersecurity incidents are attributed to insiders. Even though a more significant percentage of those threats are unintentional, healthcare service providers cannot underestimate the danger posed by the vulnerabilities. As noted in chapter two, constraints that compromise service delivery exacerbate security threats associated with IoT medical devices. The constrictions identified include resource limitation, mobility, as well as communication and data heterogeneity. Experts agree that the number one vulnerability of IoMT devices is password security and the continued use of hard-coded credentials. Sahu et al. [38] also reviewed the worm-based attacks that are characterized as a transmission channel, spreading parameters, and user mobility models. IoT users download infected files from the Internet or send and receive infected files using Bluetooth devices. Other ways of spreading worms in IoT include using infected memory card and infected files attached to MMS messages.

Health organizations struggle to address these vulnerabilities and protect devices. The reason for this difficulty is the lack of adequate training for practitioners and IT experts on the best and most secure coding practices [37]. Another reason is the pressure that system development teams face concerning meeting product deadlines. Besides, IoT vendors design some of the systems and devices to last for ten

or more years. Since many hospitals do not prioritize the need to upgrade to the latest and more secure systems, these devices are left vulnerable to new trends in cyber-attacks. Chapter one highlighted that the integrity of IoMT is a significant concern since security risks threaten the delivery of accurate and objective information. Enhancing the security of these devices is critical as it ensures that safety and effectiveness are guaranteed.

Consequences of Using Unsecured IoMT Devices

Using IoMT devices when patient data is not secured can result in adverse consequences for all stakeholders in the health sector. As noted in chapter one, the health industry is heavily reliant on information, meaning that in the event of compromised data, it may affect subsequent processes and intervention strategies. A security breach of healthcare information may lead to loss of privacy and confidentiality, as well as wrong prescriptions, diagnosis, and treatment plans. These outcomes may translate to adverse medical consequences, even contributing to death. Moreover, if IoMT devices are not secure, it puts sensitive patient information at risk of unauthorized access and hacking. Besides, cyber-attacks can expose patient data to the risk of being used for other malicious purposes.

Another consequence of using IoMT devices that are not secured is negative impacts on availability, a crucial element of data security. Information collected and stored by the IoT devices must remain accessible to authorized personnel at any time. However, this aspect cannot be guaranteed where devices are vulnerable to cyber-attacks. One of the activities that cybercriminals undertake is deleting critical information, rendering it inaccessible to those who need it. In this case, unsecured devices provide no guarantee that physicians and other medical practitioners will access patient information as required. Such devices will not be dependable or reliable as the lack of access can cripple service delivery and result in more adverse consequences.

Case Studies

Recently, a ransomware attack targeting a Michigan medical centre led to its closure. Hackers forced Battle Creek, a centre for ENT and hearing, to shut down after they attacked and deleted all patient records from the company system [39]. The hacking attack that targeted patient information from the EHR system saw the facility's medical records infected with ransomware, after which the hackers demanded \$6500 for access to the files [39]. When the management declined to pay the ransom, the hackers proceeded to delete all files and patient data records. This security incident involving patient data crippled the medical facility, leading to the closure of the centre and patient outcry.

Another incident happened in a heart clinic based in Melbourne after hackers scrambled patient information in what was confirmed later as a ransom attempt. It is believed that the malware used to

penetrate the security network at the hospital originated from Russia or North Korea. The attackers encrypted patient data at the facility, making it inaccessible to any other person [39]. Despite acknowledging that the security of their patients is the hospital's primary concern, they admitted to the data breach, illustrating just how much the health sector has become a target for cybercriminals. In both incidents, the costs to patients and the healthcare sector were enormous.

The Need for Security Solutions

As discussed above, there is a problem with IoMT devices due to the security concerns associated with them. As such, there is an urgent need for security solutions. Numerous research studies have acknowledged this fact and agree that the future of IoT medical devices rests on how users address the current security issues. The review on patient data threat conducted in this chapter has revealed that to understand the data threats better. Analysis needs to be undertaken based on secure IoT architecture, as derived from literature. The next section defines each layer of the IoT architecture.

IoT Architecture, Security Requirements, and Technologies

IoT Perception Layer Cyber Threats

The perception layer is the lowest level in conventional IoT architecture. Its primary objective is to gather useful information from the environment using things such as sensors, heterogeneous devices, and WSN. After collecting valuable data, the perception layer transforms it into a digital set-up. This layer is considered the brain within an IoT architecture, as its primary responsibility is to secure the transmission of data. Several sources have been identified to provide information about cyber-attacks and solutions within the perception layer. In their study, Asare et al. [40] analyse the hybrid cryptographic algorithm that can be applied as a solution for the vulnerabilities of the perception layer. The authors focus on frameworks that enhance data security in node communication. Tenorio et al. [41] present a discussion of low-cost Smart Meter Solution to cybersecurity threats targeting the perception layer. Their author narrows down on the meter solution based on Raspberry pi 3 and its effectiveness against untrusted cloud providers. The other source identified is [42], who proposed the use of a PPDA scheme in edge computing. According to this source, the best solution for message attacks on computer systems is a formal proof that provides data storage efficiency. On their part, Karmakar et al. [43] state that there is a temporal relationship between data located within specific time-windows. They analyse the pervasive security measures that can be used as a defence against cyber-attacks.

Wang et al. [44] clarify the dangers of cybersecurity threats such as privacy attacks. In solving this type of vulnerability, the author states that Balance PIC is the best and most effective framework when it comes to preserving privacy, costs, and integrity. Meanwhile, Wu et al. [45], maintains that collusion

attacks can be solved by employing the use of a multi-authorization centre. This will help to promote data storage security using flexible access control and partial decryption measures. On the other hand, Jiang et al. [46] discuss the SHE scheme as an efficient data security solution for the evaluation of multiple data. According to them, the best solution for data confidentiality attacks is an efficient SIMD homomorphic comparison. As for Tripathi et al. [47], their analysis is focused on solutions to false data injection attacks using ElGamal encryption and identity-based signature scheme.

Another study reviewed is [48], which provides an analysis of health data privacy schemes. In their article, they reiterate that an aggression scheme is necessary to address differential attacks and confidentiality disclosure. Saha et al. [49] narrowed their data security discussion to analyse the role of White-Box cryptography in data encryption. As explained in this article, differential attacks and code-lifting can be solved through the cipher block chaining mode associated with White-box Cryptography. Li et al. [50] study state that the best solution against data privacy and authentication attacks in mobile edge computing is the privacy-preserving data aggregation scheme. Specifically, their main point is that the data aggregation scheme is a practical solution against cyber threats such as the coalition, malicious tampering, and ciphertext attacks. The other article is by Tao et al. [51], who recommend the use of the Secure Data scheme to prevent data breaching and collusion. The authors of [52] and [53] analyse IoT systems and offer insight into data integrity and sensor-cloud architecture, respectively. The two sources agree that the best solutions against data tampering, modification, and Denial-of-Service (DoS) attacks, are random time hopping sequences and multi-layer client-server models. Lastly, Lu et al. [54] have been consulted to provide information about the effectiveness of Fog computing in enhancing data security.

Chaudhry et al. [55] recommend that healthcare providers using IoT technology should be worried about security, which incorporates burglary or loss of devices, conceivable infection contamination, conceivable unapproved movement interference, among other issues. IoT devices require privacy, validation, and control. Chaudhry et al. [55] give a brief of the current security challenges on IoT devices and their prevention techniques, which mainly focus on the perception layer.

Meena et al. [56] introduce a new attack called the Sybil attack. The attack subverts system network reputation by creating many pseudonymous identities and gaining a significant influence on user data. They outline how the privacy of patients' data can be enhanced by using re-encryption techniques in permissioned Blockchain systems. By using proxy-based re-encryption, this will provide the required access control to patients over their data.

Muhtasim et al. [57] shed light on how Secure Transaction can be established in IoT Devices by applying Blockchain technology to contain a denial-of-sleep attack. According to [57], denial of sleep

attacks are attacks on hardware devices which drain the device power source making it to malfunction. They propose the use of an encryption technique to address this attack. On the other hand, Cao et al. [58] offer a fast authentication data transfer technique for NB-IoT devices in a 3GPP 5G Network platform. This can help suffice impersonation attacks by using Canetti–Krawczyk Model. This model analyzes the problem of security authentication using key agreement protocols. The author also casts light on the traditional EPS-AKA access authentication mechanism, which continues to be a challenge in combating impersonation attacks.

Abdulrahman et al. [27] mention that IoMT forms part of tools for implementing clinical medical records (CMR). The CMRs are distributed across originating clinical centres or client-side. Hence, there is a need to collect patient records in a centralized data centre (server) while ensuring the privacy of patients' information. The authors present strategies for addressing these challenges systematically. In this case, CMRs are subject to anonymization by removing patient-identifiable information and performing pseudonymization on the unique patient ID via one-way hashing. The following table (table 3) indicates the threats.

Table 3: IoT Perception Layer Cyberthreats

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Asare et al. 2019 (101) [40]	The article aims at recommending a hybrid cryptographic algorithm to enhance data security for node communication within an IoT system.	Disruptive distributed denial-of-service attacks, impersonation attacks and man-in-the-middle attacks	Hybrid cryptographic algorithm.	To make sure a hybrid cryptographic scheme exchange data between nodes securely
Tenorio et al. 2020 (1) [41]	Presenting a low-cost Smart Meter solution based on Raspberry pi 3	Physical (local) data tampering attacks, eavesdropping, and data tampering.	Low-cost Smart Meter for secure data acquisition, transfer, and ciphering	Best security the solution in case the adversary can bypass the reliable execution capability
Zhang et al. 2020 (4016) [42]	Proposing a PPDA scheme for edge computing.	Message attack (EU-CMA)	Lightweight and verifiable PPDA scheme (LVPDA)	Additional research on computational cost comparison
Karmakar et al. 2019 (2573) [43]	The authors represent the temporal relationship between data within a specified time window.	Man-in-the-middle attack	Encryption, data integrity, and access control	IoT application in the creation of smart cities
Wang et al. 2019 (2679) [44]	Proposing BalancePIC as a scheme for preserving the integrity, costs, and privacy.	Privacy attacks	BalancePIC	The limitations of other schemes that can be overcome by BalancePIC

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Wu et al. 2019 (764) [45]	Proposing a multi-authorization centre to achieve data storage security.	Collusion attack	Partial decryption and flexible access control with attribute revocation.	Application of Smart grid in ensuring data security
Jiang et al. 2019 (10177) [46]	Provide the first instance of an efficient SHE scheme to evaluating multiple data.	Data confidentiality attack.	Efficient SIMD homomorphic comparison.	Effectiveness of lattice-based cryptography in preserving data confidentiality in the healthcare sector
Tripathi et al. 2018 (187) [47]	Proposing a secure scheme for data aggregation.	False data injection attacks	ElGamal encryption and an identity-based signature scheme	Costs of each computation involved in IoT devices, fog nodes, and the cloud
Tang et al. 2019 (8714) [48]	Analyzing a privacy-preserving scheme for health data.	Confidentiality disclosure and differential attacks	Aggregation scheme and Boneh–Goh–Nissim cryptosystem	The concept of differential privacy and its limitations
Saha et al. 2019 (637) [49]	Presenting a solution to overcome problems associated with unprotected devices.	Entropy Attack, Differential Computation Attack (DCA), Code lifting and differential attacks	White-box Cryptography that enhanced cipher block chaining mode	Protection against external encoding inversion.

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Li et al. 2018 (4755) [50]	Discussing the concept of privacy-preserving in the context of data aggregation.	Coalition attack, malicious tampering attack, ciphertext attack	Privacy-preserving data aggregation scheme	The concept of ciphertext attacks and how they are carried out
Tao et al. 2018 (410) [51]	Analyzing IoT systems using secured hardware-based data collection	Data collusion, and data breaching	Secure Data scheme	The efficiency of hardware-based security systems
Aman et al. 2018 (3102) [52]	Analyzing IoT systems in terms of low power data integrity	Modification attacks and data tampering	Random time hopping sequences	The concept of a random permutation
Kakanakov et al. 2017 (1001) [53]	Discussing the Sensor-cloud architecture that integrates the native ingredient of security	Denial of Service (DoS) attacks privacy and protection.	Multi-layer client-server model, gateways, sensors, and servers	Big Data tasks in complex systems.
Lu et al. 2017 (3302) [54]	Discussing the effectiveness of Fog Computing in enhancing the privacy of data in IoT systems	Differential attacks, data injection attack, Denial of Service (DoS) attacks.	Lightweight Privacy-preserving Data Aggregation	What are the recent trends in Fog computing?
Abdulrahman, et al. (2014) [59]	The article outlines possible attacks and their possible solutions.	Eavesdropping, replay attack, exhaustive search attack, burn attack, insider attack, physical threat	Anonymization of the personally identifiable information of patients using cryptographic techniques and pseudonymize the unique patient ID and transmit the	Unless mitigated, it may lead to a range of adverse consequences such as redundant orders of the messages

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
			data to a centralized data repository for secondary analytics using hybrid encryption technique	
Kumar, et al., (2016) [60]	The article proposes a lightweight Data Security Model for IoT Applications.	Brute force attack.	Using a 128-bit key sufficient to resist brute force attack	Related issues based on data encryption
Chaudhry (2018) [55]	The author gives a brief of the current security challenges on IoT devices by presenting different security attacks and their prevention techniques in detail, with their pros and cons.	An interloper hacks IoT sensors to access singular information. Physical attacks, including spoofing, listening in, sticking, no dereplication attacks	Data encryption must be associated with sensor or customer affirmation. Utilize straightforward protocol with a capacity of scrambling information with the private key.	
Meena et al. (2019) [56]	The author outlines how a patient's privacy can be ensured using proxy re-encryption in permissioned Blockchain	Sybil attack	Using proxy re-encryption to give access control to the patient over his data	

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Muhtasim, et al., (2018) [57]	The article focuses on Secure Transaction in IoT Devices Using Blockchain technology.	denial-of-sleep attack	Using encryption	Introducing the concept of machine learning and data mining,
Cao et al. (2018) [58]	The article focuses on Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network	Impersonation attacks	Using Canetti–Krawczyk Model to analyze the security of authentication and key agreement protocols	Use of traditional EPS-AKA access authentication mechanism

IoT Network Layer Cyber Threats

The network layer has the responsibility of connecting to smart things, servers, and network devices. The features of this layer in the IoT architecture are used in the transmission and processing of data from sensors. For information about IoT Network Layer cyber threats, some sources, as discussed in the previous sections were used. Nonetheless, one additional reference used is by [61]. This study offers a case study of the iOS devices and the association with data exfiltration. The authors conclude that pairing modes can be utilized to address data exfiltration by establishing a trusted relationship between personal computers and iOS devices. In Suo et al. [62] study, the types of attacks identified include Denial of service, counterfeit, and Man-in-the-Middle Attacks. While conducting a review of security issues in IoT networks and systems, the article finds that measures such as cryptographic algorithms and encryption mechanisms can be applied in addressing the system vulnerabilities. Sachdev et al. [63] also identified man-in-the-middle attacks as a threat on the volume, variety, and velocity of healthcare information. The authors proposed RC4 encryption as a security measure that incorporates variable-length cipher strength via a proposed PRGA key rotation method.

Goel et al.[64] explains that the healthcare industry must employ the use of tamper-proof record systems to deal with tampering attacks. Mail et al. [65] offer useful information regarding the frameworks for sharing data via industrial IoT. In this case, their proposed solution for insider keyword guessing attack is outsourced decryption.

Lee et al. [66] describe the IoT systems in healthcare systems. The authors accept that medical information is vulnerable to replay attacks. The proposed solutions entail installing the WBAN Security framework. Wang et al. [44] is another study That offers insight into the usefulness of Balance PIC as a solution to privacy attacks. As explicated in the article, this framework works by establishing a threshold on IoT device loads.

Khandare et al. [67] focused on encryption techniques to protect patient privacy in healthcare systems. They note that public area network is used to send data from healthcare devices to the cloud, and it is not secure. According to them, in this case, hackers can attack, read, and modify the data in public during transmission. They [67] also propose the use of access control based on encryption and cryptography to protect the privacy of patient's data. In their study, the authors reviewed the different models, schemes, as well as implementation related to data encryption and cryptography algorithms proposed by various researchers to secure smart wearable medical healthcare devices. However, the authors state that the solution does not secure inside attacks. In this effect, Al Asli et al. [68] proposed a new scheme using Field Programmable Gate Arrays (FPGAs) to secure IoT data processing in public clouds

against a wide range of threats, including the insider attacks. In their proposed solution, FGPA authentication, the authors recommend a secure way to establish a symmetric session key between the on-cloud FGPA, the IoT device, and the client. The solution allows the user's configuration integrity check while running in the cloud FGPA. Vijayalakshmi et al. [69] further propose a hybrid security technique based on obfuscation and encryption technologies to prevent healthcare data from attackers and unauthorized users (insiders) during transmission.

Purohit et al. [70] propose a remedy to DoS attacks by using a hybrid method of securing communication between IoT devices using data confidentiality and authentication. The hybrid solutions will efficiently encrypt device to device communication using the Radix-64, which is easy to decrypt at the end. Bhattacharjee et al. [71] also proposed a hybrid approach for securing IoT communication using the radix-64 conversion RSA algorithm and radix-64 conversion hash function.

Al Breiki et al. [72], on the other hand, sheds light on Decentralizing Access Control, which, if used in IoT networks and devices, can help contain reentry attacks. Decentralized access control can be effectively deployed using Blockchain and other Oracles related techniques. This ensures that transactions are entirely executed and the value transfer made before the next transaction is processed. This disallows cases of fraud during a transaction. They [72] also proposed a decentralized access control of IoT data using blockchain and trusted oracles. The solution employs smart contracts to achieve decentralized access control to allow end-users to access remotely stored IoT data. Pankomera et al. [73] also discussed how vulnerabilities and threats could be mitigated in managing the security of health information in a patient-centric context, specifically in a resource-constrained setting. The authors proposed that a comprehensive approach should comprise of devising customized solutions that meet the local needs of patient-centric systems, such as access control.

Liu et al. [74] remark that the exponential growth of devices connected to the network has resulted in the development of new IoT applications such as IoMT, which have diverse requirements. The authors note that the emerging software-defined network approach can be leveraged for the IoT environment to help users achieve differentiated quality levels. However, the solution is prone to spoofing, which is solved using an SDN-based data security model based on a middlebox-guard (M-G) that aims at reducing network latency and enhancing security.

Pallavi et al. [75] state that IoT proliferates and performs better than many other technologies. The technology consists of constrained sensor-based devices that are connected to communication. The sensors produce a considerable quantity of data that should be confidential in many cases. In effect, different sorts of lightweight cryptographic algorithms for secure data transmission is used. Each

algorithm has a different performance based on its key size, rounds/cycles, and storage. The authors recommend that the cryptographic algorithms used for the IoT devices should have various considerations for the better performance of the device as well as for keeping security as a priority.

The table 4 shows security issues in the IoMT network layer, as well as the proposed security solutions.

Table 4: IoT Network Layer Cyberthreats

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Asare et al. 2019 (101) [40]	To discuss the concept of data exchange within IoT systems between nodes that use DHE and TwoFish.	Security breaches that happen in hardware set-ups	Cryptographic algorithms that prevent unauthorized access to data	Diffie-Hellman Key Exchange Protocol.
Tenorio et al. 2019 (1) [41]	Analyzing support for IoT data sources using low-cost, practical data	Data acquisition and transmission	Raspberry Pi 3	Application of Smart Meter within an IoT infrastructure
D'Orazio et al. 2016 (524) [61]	Case study of iOS devices and data exfiltration from IoT.	Data Exfiltration from unsafe applications on devices	Pairing mode. IoT vendors should provide mechanisms that allow users to selectively authorize a client software to access device resources on the user's behalf. Users should avoid installing applications from an unknown origin.	Demonstrate how data exfiltration occurs in a practical setting.
Suo et al. 2012 (648) [62]	Conducting a review of security in the Internet of Things	Denial of service, counterfeit attack, Man-in-the-Middle Attack	Encryption mechanism, communication security,	Why intelligent processing is limited for malicious information

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
			cryptographic algorithms	
Goel et al. 2019 (25) [64]	Developing a tracking system for a tamper-proof record using patient blockchains and healthcare authority	Tampering attacks on healthcare records	Blockchain technology	Role of data repository in addressing the limitations of the existing models and solutions
Aman et al. 2018 (3102) [52]	Analyzing IoT systems in terms of low power data integrity.	Cyber-attacks such as modification attacks and data tampering	Random time hopping sequences that detect data tampering in IoT network systems	The concept of a random permutation
Miao et al. 2019 (8681) [65]	Discussing the framework for data sharing through industrial IoT	Insider keyword guessing attack.	Encryption and outsourced decryption	The researchers recommend extending the data-sharing framework to reduce computation cost for DO during offline encryption by using optimized pairing-based cryptographic accelerators embedded in IoT devices
Lee et al. 2014 (453) [66]	Analyzing medical patient medical information in healthcare systems	Replay attack.	WBAN Security	The authors propose the implementation and experimentation using their key

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
				management scheme to improve the ability of analysis.
Wang et al. 2019 (2679) [44]	Proposing BalancePIC as a scheme for preserving integrity, costs, and privacy.	Privacy attacks	Putting a threshold on computational costs and IoT device loads.	Importance of trust discovery.
Li et al. 2018 (4755) [50]	Discussing the concept of privacy-preserving on the context of data aggregation	Collusion attack.	Mobile edge computing	Mobile edge computing in data privacy
Saha et al. 2019 (637) [49]	Presenting a solution to overcome problems associated with unprotected devices.	Code lifting and differential attacks	White-box Cryptography.	Block cipher in IoT.
Zhang et al. 2020 (4016) [42]	Proposing a PPDA scheme for edge computing.	Message attack (EU-CMA)	Formal proof for providing efficiency in data storage and computational services	Role of data aggregation in IoT cybersecurity
Wu et al. 2019 (764) [45]	Proposing a multi-authorization center to achieve data storage security.	Collusion attack.	Partial decryption and flexible access control	Smart grid and how it is applied in ensuring data security
Jiang et al. 2019 (10177) [46]	Provide the first instance of an efficient SHE scheme to evaluating multiple data.	Man-in-the-middle attack	SIMD homomorphic comparison.	How lattice-based cryptography preserves data confidentiality.

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Karmakar et al. 2019 (2573) [43]	Representing the temporal relationship between data within a specified time window.	Cyberattacks	Trust evaluation	Importance of data trust in IoT systems
Meena et al. 2019 (450) [56]	Proxy re-encryption in permissioned Blockchain	Data breach	Public Key Infrastructure (PKI) and hyper ledger fabric and ensuring that patient's medical records are in complete control of patients only	Further research on design and deployment of Proxy re-encryption
Tang et al. 2019 (8714) [48]	Analyzing a privacy-preserving scheme for health data.	Confidentiality disclosure and differential attacks	Aggregation scheme	The concept of differential privacy.
Pankomera et al. (2017) (4) [73]	The article identifies the ten most critical web application security risks	Function-Level Access Control Attack, injection, broken authentication, cross-site scripting, insecure direct object referencing, security misconfiguration, sensitive data exposure, using components with known vulnerabilities	Enforcing mechanism to deny all access by default, requiring explicit grants. Keeping untrusted data separate from commands and queries, encryption and use of strong passwords for IoMT solutions	Attackers using authorized system users can still change URLs or parameters to run a privileged function.
Liu et al. (2017) [74]	The article presents an SDN-Based Data Security solution for Internet of Things	VLAN tag spoofing.	Use of an SDN-Based Data Security model.	Issues of Scalability with the proposed model

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
			The model is based on Middlebox-Guard (M-G) that aims at reducing network latency	
Goel, et al., (2019) [64]	The article addresses Blockchain data security in IoT Server Platform	DoS (Denial of Service) attacks	Using the encryption method and the authentication method of Ethereum blockchain	Complexity in systems operating blockchain algorithms
Suo, et al., (2012) [62]	The article addresses security in the Internet of Things.	Distributed denial of service attack (DDoS)	Identity authentication and use of anti-DDOS	Preventing the DDOS attack for the vulnerable node is another problem to be solved.
Khandare et al. (2019) [67]	Reviewing different models, schemes, as well as implementation related to data encryption and cryptography algorithms proposed by various researchers to secure smart wearable medical healthcare devices	Cyber attackers reading and modifying data in the network during transmission while used public area networks for IoMT	Protect the privacy of patient's data using access control mechanisms based on encryption and cryptography	This solution cannot prevent inside attack but shields data during transmission
Al-Asli (2018) [68]	The researchers propose a new scheme using field-programmable gate arrays (FPGAs) to secure IoT	Insider attacks, impersonation, and man-in-the-middle attacks.	FGPA authentication – a secure way to establish a symmetric session key between the on-cloud FGPA, the IoT device, and the client. The solution	

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
	data processing in public clouds against different attacks		allows the user's configuration integrity check while running in the cloud FGPA.	
Vijayalakshmi (2018) [69]	The researchers identify the critical nature of data handled by IoMT and the need to ensure data confidentiality, integrity, and availability. They proposed hybrid security techniques to secure healthcare data in the devices	Unauthorized user access to healthcare data during communication	Deployment of hybrid techniques to secure healthcare data. The solution is based on data obfuscation and encryption technologies to prevent unauthorized access to personally identifiable information	The proposed solution for data transmission is not the only secure to transmit IoMT healthcare data. The researchers recommend that in future, more data transmission techniques can be applied
Al Breiki et al., (2019) [72]	The researchers note that the currently available methods for access control in IoT systems are mainly centralized. They propose a decentralized access control systems to IoT data using blockchain and trusted oracles	Reentry attack	Deployment of features of blockchain and smart contracts Ensuring complete transaction execution and value transfer before processing the next transaction	The proposed solution has not been fully designed and developed for adoption in mitigating the identified attacks
Sachdev, et al., (2016) [63]	The paper focuses on Improving Real-Time Data Streaming Security	Man in the middle attack	Use of Real-Time Data Streaming model to ensure secure transmission.	Multiple vulnerabilities discovered in RC4 like Fluhrer, Mantin, and Shamir (FMS) attack

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
	to Promote Patient and Physician Socialization			
Purohit, et al., (2017) [70]	The article proposes a Hybrid Approach for Securing IoT Communication Using Authentication and Data Confidentiality.	DOS attacks	Using hybrid solutions to encrypt IoT communication using Radix-64	Radix- 64 conversions can be straightforward for hackers to decrypt
Tao et al. (2018) [51]	The authors investigated challenges with data collection in IoT-based healthcare applications and proposed a new data collection scheme called the SecureData to provide data security and preserve the privacy of patient's data	Ransomware, DDoS attacks, insider, email compromise, eavesdropping, collusion attacks, and fraud scams	The authors offer a lightweight KATAN secret cipher algorithm in the networked sensor or devices layer	This solution requires the detailed implementation of the algorithms with various metrics and investigate the protection performance of the algorithms under threats
Bhattacharjee et al. (2017) [71]	The authors present a hybrid procedure to secure IoT communication by utilizing a radix-64 conversion hash function and radix-64 conversion RSA algorithm	DoS attacks, weak access control, data protection	Securing IoT communication using authentication and data confidentiality to address the vulnerabilities in the IoT network	The solution only secures communication, leaving the actual IoT system unattended

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Pallavi, et al., (2020) [75]	The article gives a comparative Study of Various Lightweight Cryptographic Algorithms for Data Security Between IoT and Cloud.	Side-channel attacks (work hole, eavesdropping, the man in the middle, DOS)	A Lightweight Block Cipher Klein used as a Substitution Permutation Network	The algorithms used have different types of structures.

Application Layer Cyberthreats

The application layer manages the delivery of application-specific services to users within the IoT network. As such, this layer defines the various applications that can be deployed within the Internet of Things. For example, the application layer is widely employed in the smart health sector and makes use of application systems such as HTTP, COSEM, NTP, and SSH.

According to D’Orazio et al. [61], big data technology has become accessible with the introduction of the Internet of Things devices. These objects and devices which are connected to a network such as the Internet and communicate with each other or provide information via it. When using cloud services, several parties are involved who influence the data protection aspects. Relationships arise between the cloud provider and the cloud user as well as the clients of the cloud user, whose data protection rights are affected as third parties. Therefore, a vulnerability in these IoT devices, software, or the operating system can be exploited to exfiltrate the data in these devices [61].

The concept of “Fog computing-enhanced Internet of Things” has recently garnered considerable attention. The fog devices deployed in network edges not only provide location awareness and network latency but also help improve the real-time quality of services offered by IoT networks. This has brought about an evolving threat paradigm targeting IoT devices where users such as peer-to-peer communication and worm-like self-propagation features. These risks arise from the fact that the data is stored on the provider's shared IT components outside of the company itself. Because of this exposure, they are exposed to numerous dangers and attack scenarios. In principle, access can be made from anywhere on the Internet, provided that the access code is known. Besides, security gaps and vulnerabilities can allow unauthorized access to the data. Another risk arises from the shared infrastructure. Since several customers share the physical resources, problems with the reliable separation of access rights to the data cannot be completely ruled out. The attackers identify the weaknesses of OT protocols that have existed for decades, such as DICOM, and can disrupt critical business functions. This can be countered by “privacy-preserving data aggregation” through fog computing applications proposed in the recent years [54].

Kingsford et al. [76] note that the leakage of personal health information can easily be compromised for medical insurance or medical identity theft. Healthcare service providers need to ensure privacy protection when collecting medical data for analyzing or publishing. [50] proposed a mathematical model for identity-based encryption protocol for privacy preservation of the patient data during the collection of health information for analysis.

According to [53], securing virtual instances is to manage implement and audit bottleneck in the IoT is essential as the Internet of Things poses many risks to the protection of personal data. Data

protection in IoT solutions particularly difficult due to the physical interaction between the real sensor and the virtual reflection. User companies should know this to be able to prepare a data protection impact assessment according to the GDPR. [53] identifies the rapidly growing number of IoT devices, consumer uncertainty with regard to data protection, and the data security increasing enormously with IoT devices. This shows that data security for IoT devices is not good, so the lack of trust among users is, in many cases, justified. There are various Adaptive models for use towards security in IoT with the Cloud technologies as outlined by [53].

The collection of devices under the bounds of the Internet of Things yield large volumes of sensitive data which, if compromised the lead to catastrophic losses. However, the continued use of public Internet when transferring data in IoT device networks increases their susceptibility to cyber-attacks. Data protection, AI, and IoT are changing the cloud, and cyber defence must keep pace. This becomes particularly difficult regarding shadow IT and a lack of data overview. The security concerns of cloud users are well known and have existed for years: data loss by hackers is one of the biggest concerns in Companies Success through B2B marketing around the world. Shadow IT also causes problems due to unauthorized cloud services and the lack of a clear overview of which company data is transferred to cloud applications. Although the number of security incidents in the Cloud Sponsored Post continues to rise, companies are increasingly turning to 'As a Service' offers. As a result of these attacks, data compromise and modification attacks may result in widespread damage [52].

According to Saha et al. [49], the Internet of Things phenomenal has sparked impressive economic progress. Various IT security solutions form the basis for more trust in the cloud. By implementing security measures that make it possible to regain transparency and control over data, companies can use innovative services and accelerate their business in the cloud. One reason for the necessary renewal of cloud security lies in the General Data Protection Regulation (GDPR). A paradigm shift in data protection law is that the GDPR provides comprehensive documentation, organization, and transparency obligations. The GDPR results in new obligations for cloud users and cloud providers. While the GDPR provides for shared responsibility between cloud users and cloud providers, ultimately, the companies that use the cloud are held responsible. Many IT buyers assume that they will effectively outsource the operation of their infrastructure to a trustworthy third party and that the provider will take care of everything [49].

With the rapid IoT development and the 5G techniques, a wide range of mobile devices with sensing capabilities continue to flood to facilitate access to networks, some of which are used in healthcare organizations. The past cloud computing architecture cannot satisfy all the requirements for fast data access and low latency in IoT applications. The Internet of Things comes with the ability to

network all kinds of devices, which becomes complex for the traditional cloud. Due to the increasingly ubiquitous access to the Internet through WLAN and mobile communications, everyday devices and systems from the private and professional environment can participate in the Internet through ever smaller and cheaper computing power. As a rule, this Internet connection goes hand in hand with the fact that devices can transmit data that they collect in their location and context using sensors. Users can react to control commands through other higher-level applications and thus do something he wants. This complexity needs to be addressed with the *“Privacy-preserving data aggregation scheme for mobile edge computing assisted IoT applications”* Examples range from switching a lamp in the area of smart home to checking and controlling large wind power plants [50].

Security concerns are realized by the recent sophisticated privacy attacks, data breaching, data collusion, and data integrity experienced in health facilities. So, if there are unique risks to data protection, special protective measures must also be taken. A data protection impact assessment is also necessary, which analyzes the concrete consequences for data protection and names measures if the planned IoT project is to be implemented. There are additional risks for data protection in the cloud computing environment due to external service providers and data centres. The storage of data on external systems accessible via the Internet requires compliance with special data protection requirements. With cloud computing, companies outsource their software, applications, or infrastructure to data centres from cloud providers. The services of the providers can be accessed via the public Internet. As a result, companies save their hardware and software and do not have to operate their own data centre infrastructure to store their data. Thanks to usage-based tariff models, costs can be saved, but there are additional risks for data protection [51].

Jeon et al. [77] reveal that the conventional IoT platforms bases on traditional database technology, MySQL, is prone to injection attack and remote access utilizing the transmission method using the HTTP protocol ruling. The authors proposed the use of blockchain smart contracts on Ethereum to store and manage real-time sensor data in blocks. However, the proposed solution is still at infancy, and more work needs to be done to come up with concrete system design and development for the IoT platform that utilizes blockchain technology to enhance IoMT security. Meena et al. [56], in a similar manner, proposed the use of public key infrastructure and hyper ledger fabric and simulated workflow of the healthcare sector to ensure that patient’s records are in complete control of the patient. The solution is a blockchain framework that provides the integrity of the medical records that users can verify in the future.

Cai et al. [78] propose a data-driven security solution to be used in IoT systems that are resource-constrained as a way of monitoring and addressing sensor-hijacking attacks. Such an attack-agnostic technique system, if developed, can secure wireless IoT systems and discuss their inability to detect electrocardiogram alteration.

Fang et al. [79], to address the occurrence of cloning attacks, suggested a flexible authentication data transmission scheme that can be used in securing IOT Applications, and prevent cloning attacks. They identify the main threats here as forwarding security, key escrow resilience, and end-to-end security. The efforts of the research sought to provide secure communications between IoT devices and increase network transmission efficiency and reliability.

Lachner et al. [80] address the data protection and performance evaluation mechanisms which can be used to ensure secure transmission of IoT data in Resource-Constrained Devices. This, according to [38], can effectively contain the Flooding attacks on IoT networks and devices. By using stream ciphers, cryptographic block, hashing algorithms, signature algorithms, key exchange protocols, and message authentication codes, flooding attacks can be controlled.

Nesh et al. [81], as a way of addressing DDoS attacks among IoT networks, outline data-driven methods which could be used to characterize DDoS IoT Exploitations; they suggest that scrutinizing network data can help identify and report malicious activities as a result of a compromise in IoT devices. It is, however, a challenge to identify the root cause of these IoT exploitations. Kurera et al. [82] developed a protocol that focuses on low power IoT devices that have low processing power and relatively limited memory. The proposed protocol creates a secure passage for data transmission over the open-air network connection, such as Wi-Fi and Bluetooth on the application layer of the IoT device.

Bhattacharjee et al. [71] proposed a Bayesian framework to maintain data integrity in an IoT system under opportunistic data manipulation by an adversary. By considering an imperfect monitoring mechanism, the researchers quantified the trustworthiness of the data being collected by an IoT hub using utility values obtained by prospect theory based on a multinomial hypothesis. The mechanism monitors data collected from IoT devices by a hub in the presence of an adversary manipulating data and an imperfect anomaly monitoring mechanism. Table 5 shows the IoT layer threats.

Table 5: IoT Application Layer Cyberthreats

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Zhang et al. 2020 (4016) [42]	Proposing a PPDA scheme for edge computing.	Existential Unforgeability under Chosen Message Attack (EU-CMA)	Formal proof for providing efficiency in data storage and computational services	The authors suggested that data aggression is increasingly becoming an issue for data security researchers in IoT cybersecurity.
Suo et al. 2012 (648) [62]	Conducting a review of security in the Internet of Things	Social engineering attacks	Encryption mechanism, communication security, protecting sensor data and cryptographic algorithms	New security and privacy challenges will keep rising as the IoT extends through the traditional Internet that is prone to a wide range of cyber threats. The research needs to be extended to cover future threats to the confidentiality and integrity of IoMT.
Wu et al. 2019 (764) [45]	Proposing a multi-authorization centre to achieve data storage security.	Collusion attack	The collision attack on a cryptographic hash tries to find two inputs producing the same hash value. Partial decryption and flexible access control with attribute revocation.	It is challenging to address Smart grid applications and ensure data security within the IoT network.
Jiang et al. 2019 (10177) [46]	Provide the first instance of an efficient SHE scheme to evaluating multiple data.	Data confidentiality attack.	Efficient SIMD homomorphic comparison.	It is a challenge to identify when the confidentiality of data in the IoT device is compromised. The lattice-based cryptography preserves may not be entirely reliable in preserving data confidentiality.

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
Meena et al. 2019 (450) [56]	Proxy 3e-encryption in permissioned Blockchain	Data alteration	Public Key Infrastructure (PKI)	Proxy re-encryption is a significant challenge as it does not guarantee a solution to altered data.
Tang et al. 2019 (8714) [48]	Analyzing a privacy-preserving scheme for health data.	Confidentiality disclosure and differential attacks	Aggregation scheme to securely collect data from multiple sources.	The concept of differential privacy.
Lu et al. 2017 (3302) [54]	Discussing the effectiveness of Fog Computing in enhancing the privacy of data in IoT systems	Security Misconfiguration	Lightweight Privacy-preserving Data Aggregation to filter false data injected by external attackers	Differential privacy and how it applies within an IoT infrastructure
Tao et al. 2018 (410) [51]	Analyzing IoT systems using secured hardware-based data collection	Injection	SecureData scheme that tackles security concerns.	The efficiency of hardware-based security.
Karmakar et al. 2019 (2573) [43]	Representing the temporal relationship between data within a specified time window.	Sensitive Data Exposure	Trust evaluation and other pervasive security measures	Importance of data trust in IoT systems
Kakanakov et al. 2017 (1001) [53]	Discussing the Sensor-cloud architecture that integrates	Phishing	A multi-layer client-server model that separates virtual and physical gateways, sensors, and servers	The shortcoming of physical interaction of virtual reflections and real sensors

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
	the native ingredient of security			
Pankomera et al. (2017) (4) [73]	The article focuses on the Applicability of 10 most critical web application security risks to patient-centric systems	Redirects and Forwards	Avoid following redirects and forwards. Ensure that the supplied value is valid and authorized for the user.	Such redirects to central systems may lead to significant data compromise of privacy
Kingsford, et al. (2017) [76]	The article addresses a Mathematical Model for Hybrid Systems for Privacy Preservation in Patient Health Records	Ciphertext attacks & plaintext attack.	Using the proposed Mathematical Model for Hybrid Systems for Privacy Preservation	The size of Healthcare data is a significant problem in Healthcare Information Systems.
Abulrahman et al. (2014). [59]	The article identifies the critical security risk related to IOMT	Exhaustive search attack	The article proposes that the best solution to these attacks is encryption techniques.	Sophisticated attacks may still bypass poor encryption techniques.
Jeon et al. 2018) [77]	The researchers propose a new IoT server platform by introducing a blockchain and store sensor data in a blockchain	The researchers mention the vulnerability of MySQL. The vulnerability is a	The solution involves the use of blockchains in the IoT platform (smart contracts), instead of using MySQL that is prone to attacks	Currently, there is no concrete system design and development based on the proposed solution.

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
		deodorization method using the SQL injection and remote access		
Cai, et al., (2017) [78]	The article addresses Data-Driven Security Solutions deployed in Resource-Constrained IoT Systems	sensor-hijacking attack	Developing an attack-agnostic way to secure the IoT systems	Inability to detect alteration of electrocardiogram
Fang, et al., (2020) [79]	The article proposes a Flexible and Efficient Authentication and Secure Data Transmission Scheme in IoT Applications	cloning attacks	Forward security, end-to-end security, and key escrow resilience	For future work, may consider providing security with communications between devices to increase network transmission efficiency and reliability.
Kurera et al. (2018) [82]	Node-to-Node Secure Data Transmission Protocol for Low-power IoT Devices	DoS attacks and MR attacks	A secure data transmission protocol for low-power IoT devices, with features in Kerberos and one-time password concepts	
Lachner et al. (2019) [80]	The article focuses on Performance Evaluation and Data Protection Mechanisms	Flooding attacks	Using cryptographic block and stream ciphers, hashing algorithms, message	Limitations and throughput rates.

The first author of the article and year	The objective of the article	Attacks category (Attacks name)	Solution (Technique)	Issues need further addressing
	for Resource-Constrained IoT Devices		authentication codes, signature algorithms, and key exchange protocols	
Neshenko, et al., (2018) [81]	The article focuses on Data-Driven techniques for Characterizing IoT Exploitations	DDoS attacks	Scrutinizing network telescope data to report on malicious activities generated by compromised IoT devices	investigating the root cause of such IoT exploitations,
Sahu, et al., (2019) [38]	This article focuses on Challenges and Issues in Securing Data Privacy in IoT and Connected Devices.	Break-in attacks, Botnet and user-based attacks, Worm-based attacks,	Use of Authentication Methods and encryption.	An intruder may easily interfere with the devices due to its limited functionality which may cause a massive data breach
Bhattacharjee, et al., (2017) [71]	This article focuses on Preserving the Integrity of data in IoT Networks through Opportunistic Data Manipulation.	On-off attacks	Using the CWMA to reflect the behavior of the node	The imperfect monitoring mechanism may compromise the trustworthiness of data.

Summary

The IoT architecture is comprised of three primary layers, each with a different set of components and functions. Understanding the structure and underlying aspects of each segment is key to developing highly secure IoT systems. Notably, all three layers have a certain degree of vulnerability that compromises data security. The tables (3, 4, and 5) included in this discussion have illustrated that each layer has specific threats and solutions that can be applied to address these security concerns. Chapter 4 is of significant implication as it provides useful information on data security in an age where the health sector is increasingly adopting the use of IoT medical devices.

Chapter 5 : Challenges and Solutions

Introduction

In this chapter, all review results from chapter 4 are discussed in detail. The chapter analyses the security threats affecting patient electronic health records collected and processed using IoMT. The chapter also highlights the discovered countermeasures, controls, and solutions to mitigate the identified security threats. Finally, the chapter outlines the challenges that healthcare institutions face when securing health records in medical IoT devices. The results of the research are analysed and presented in the form tables, charts, and graphs. Text is used to introduce tables and figures and guide the reader through an analysis of the results. The structure of the chapter is as shown in figure 3:

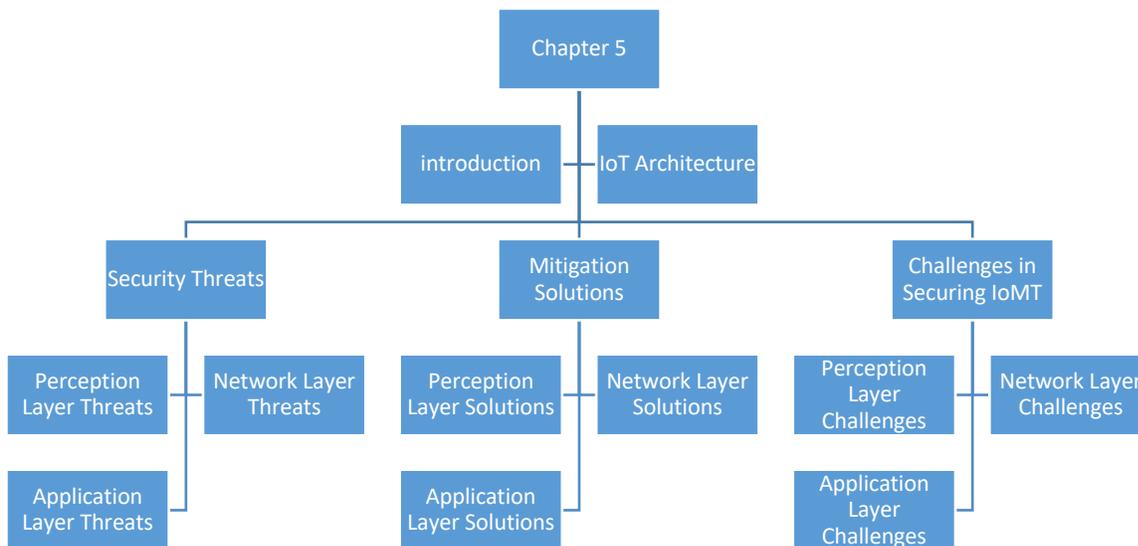


Figure 3: Discussion chapter structure

The Three Layers of IoT Systems

Chapter four reveals that the most basic architecture for IoT systems is a three-layer architecture, namely the perception, network, and application layers, as shown in figure 3. The perception layer is the physical layer composed of IoT sensors for detecting and collecting information from an environment. The layer identifies physical parameters or other smart objects in the environment. The network layer, on the other hand, connects IoT devices to other smart things, network devices, and servers. The segment plays a crucial role in transmitting and processing IoT sensor data. Finally, the application layer delivers application-specific capabilities to end-users. The layer defines the various applications in which users can deploy IoT, for instance, in medicine, smart cities, and smart homes.

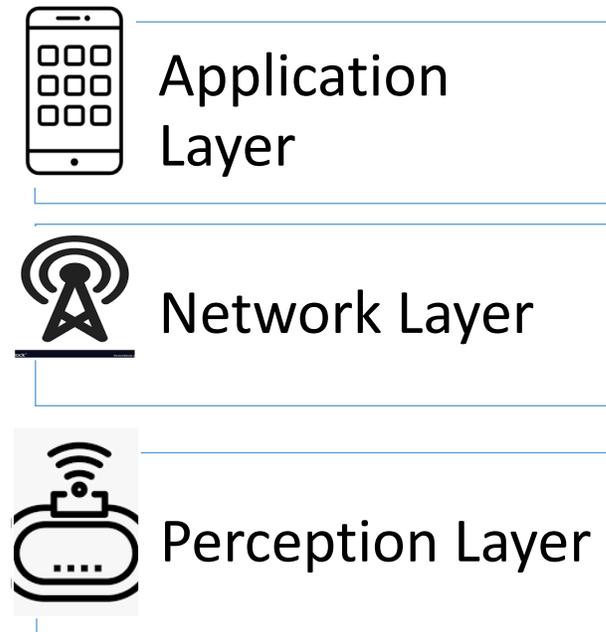


Figure 4: IoT Architecture

Security Threats Affecting Patient Electronic Health Records in IoMT

What are the security threats affecting patient electronic health records collected and processed through medical wearables and sensor-based IoT devices, and cloud information management? What are the IoT layers threats, and how do they compromise data privacy and security? To respond to the research question, this section of the chapter is divided into three parts, each representing a specific layer of the IoT architecture.

IoT Perception Layer Security Threats Analysis

Table 6 features a summary of the threats or attacks targeting the perception layer. As mentioned, the perception layer is the lowest level in conventional IoT architecture with a primary objective of gathering useful information from the environment using sensors, heterogeneous devices, and wireless sensor networks. Information collected in the perception layer is transformed into a digital set-up. Chapter four identified several sources to provide information about cyber threats and solutions within the perception layer. Table 6 shows a summary of the identified risks in the perception layer:

Table 6: Summary of Threats/Attacks in the Perception Layer

Threat/Attack	Description	References
Distributed denial of service attacks (DDoS)/ Denial of sleep attack (DoSL)	Denial of service attacks launched from multiple locations simultaneously	[40, 53, 54, 57]
Man-in-the-middle attacks/Eavesdropping	An attempt to traverse information of a communication link between the IoT device and server. The act of stealthily listening to private communications without the sender and receiver's consent.	[40, 43, 59]
Physical (local) data tampering attacks	Accessing IoT devices and deliberately modifying, manipulating, or editing the data.	[41, 42, 55, 59]
Privacy/Collusion Attacks/Data confidentiality attack/Confidentiality Disclosure/Differential Attacks	An IoMT device is illegally accessed or compromised by an adversary in a way that is hard to detect.	[44-46, 48-52, 54, 55, 58]
False data injection	Compromising reading of multiple sensors to mislead the systems and users	[47, 54]
Brute force attack and Sybil Attack	Using trial and error by working through numerous possible combinations to guess user credentials.	[56, 60]

The articles reviewed in chapter four identified a total of twenty-six attacks in the perception layer of IoT. Privacy/Collusion Attacks/Data confidentiality attack/Confidentiality Disclosure/Differential Attacks were the primary attacks identified by most of the reviewed articles, being mentioned in 11 times out of the 26 IoT perception layer attacks identified, as shown in figure 5.

Both physical/local data tampering and DDoS/DoSL attacks were mentioned four times each, while man-in-the-middle attacks were mentioned three times. Other security threats that the research identified include brute force attacks and false data injection.

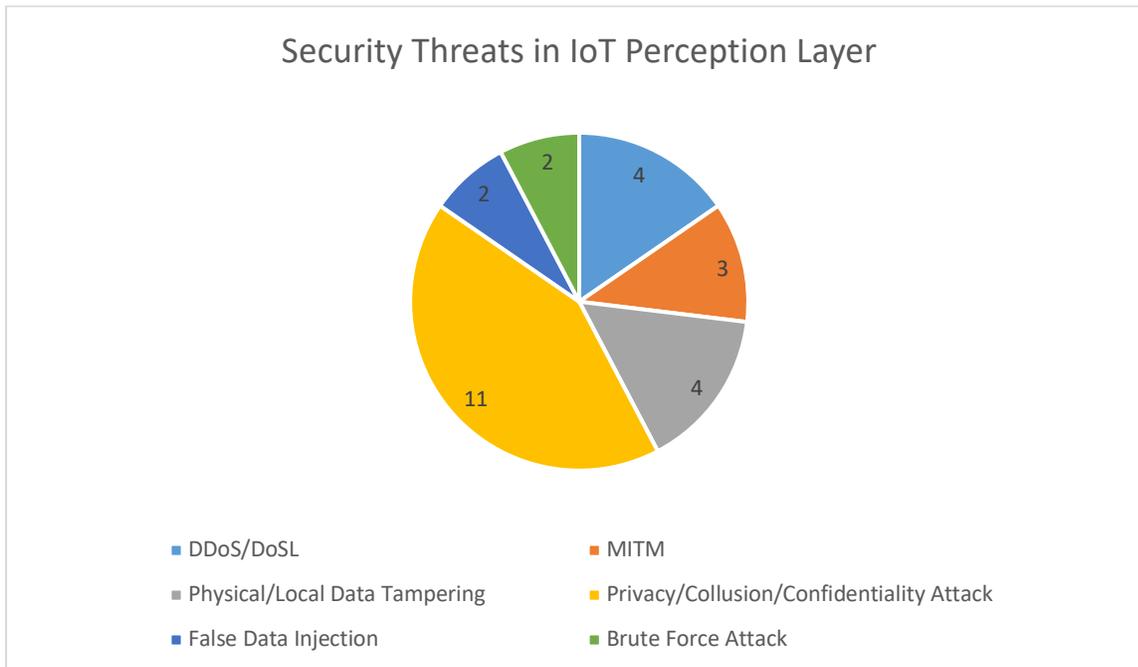


Figure 5: Summary of IoT Perception Layer Security Attacks

IoT Network Layer Security Threats Analysis

The network layer is responsible for connecting smart things, servers, and network devices. This IoT layer has features used for transmitting and processing data from sensors. Table 7 summarizes the common security threats identified for the network layer.

Table 7: Summary of Threats/Attacks in the Network Layer

Threat/Attack	Description	References
Hardware misconfiguration	Security breaches that happen due to wrong or poor hardware set-up	[40]
Data exfiltration/Tampering attacks/Message attacks	Stealing data during transmission from unsafe applications on IoT devices. Modification attacks that tamper with healthcare data transmitted by IoMT systems	[41-43, 52, 56, 61, 64, 67, 69]
Denial of service attack	Denial of service attacks launched from multiple locations simultaneously	[62, 64, 70, 71, 75]
Man-in-the-middle attack/ Replay Attack/ Eavesdropping	An attempt to traverse information of a communication link between the IoT device and server. The act of stealthily listening to private communications without the sender and receiver's consent.	[46, 51, 62, 63, 66, 68, 72]
Brute force attacks/insider keyword guessing	Using trial and error by working through numerous possible combinations to guess user credentials.	[65]
Privacy attacks/Collusion attacks/ Code lifting and differential attacks/ Confidentiality disclosure	An IoMT device is illegally accessed or compromised by an adversary in a way that is hard to detect.	[44, 45, 48-51]
Injection attack	Compromising reading of multiple sensors to mislead the systems and users during data transmission	[73]
Spoofing attacks, email compromise	A malicious party impersonates another device or user on a network to launch attacks against network hosts, bypass access controls, steal data, and spread malware	[51, 74]

Chapter four identified eight main categories of security threats targeting the IoT network layer. They include Hardware misconfiguration; Data exfiltration/Tampering attacks/Message attacks; Denial of service attack; Man-in-the-middle attack/ Replay Attack/ Eavesdropping; Brute force attacks/insider keyword guessing; Privacy attacks/Collusion attacks/Code lifting and differential attacks/Confidentiality disclosure; Injection attack; and Spoofing attacks/Email compromise. IoT Network security threats were mentioned 32 times in the articles reviewed in the research. An analysis of the results indicates that data exfiltration/tampering attacks were mentioned in 9 of the 32 times, as shown in figure 6.

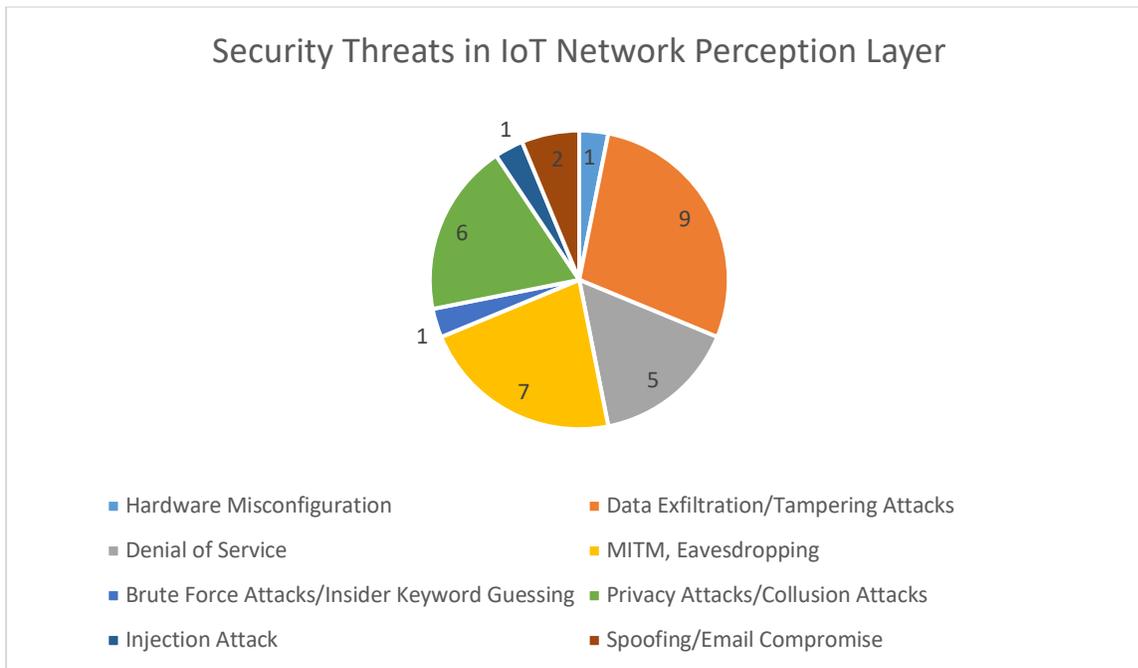


Figure 6: Summary of IoT Network Layer Security Threats

Man-in-the-middle attacks and eavesdropping was mentioned seven times in the articles reviewed, while privacy/collusion attacks were mentioned six times. Denial of service attacks was identified in five articles while spoofing, and email compromise threats were addressed in two articles. Hardware misconfiguration, brute force attacks, and injection attacks were reviewed in one article each.

IoT Application Layer Security Threats Analysis

The application layer manages the delivery of application-specific services to users in the IoT network. The introduction of IoT systems has made big data accessible to end-users. However, malicious criminals have discovered ways to exploit vulnerabilities in IoT devices, software, or operating systems to exfiltrate data in IoT systems. Table 8 summarizes the common security threats identified for the IoT application layer.

Table 8: Summary of Threats/Attacks in the IoT Application Layer

Threat/Attack	Description	References
Data exfiltration/Tampering attacks/Message attacks	Stealing data during transmission from unsafe applications on IoT devices. Modification attacks that tamper with healthcare data transmitted by IoMT systems	[42, 76]
Social Engineering attacks/Phishing	Use of deception to manipulate unsuspecting users into divulging personal information to hackers for fraudulent use	[53, 62]
Privacy Attacks/Collusion Attacks/Data confidentiality attack/Differential Attacks	An IoMT device is illegally accessed or compromised by an adversary in a way that is hard to detect.	[43, 46, 48, 56]
Security misconfiguration	Failure to implement all the security controls for IoT applications, or to implement security controls with errors	[54]
Injection attacks/ Redirects and forwards	Compromising reading of multiple sensors to mislead the systems and users during data processing in IoMT applications. Web applications accept untrusted input, causing the web application to redirect the request to a URL contained within untrusted input	[51, 73, 77]
Brute force attack/Exhaustive search attack	Using trial and error by working through numerous possible combinations to guess user credentials	[59]
Sensor hijacking attacks	Hackers target IoMT devices and make them generate arbitrary user health state information.	[78]

Cloning attacks	Physical capture attacks where an adversary launches clone attacks by replicating the compromised nodes [79]
Denial of service/Flooding attacks/Botnets/Worm-based attacks	Denial of service attacks launched from multiple locations simultaneously [38, 80-82]
On-off attacks	Malicious nodes opportunistically behave good or bad, compromising the network while hoping that the bad behaviour will not be detected [71]

Chapter four identified ten major attacks targeting the IoT application layer. They include data exfiltration and tampering attacks mentioned in two articles; social engineering and phishing attacks mentioned in two papers; privacy attacks/collusion attacks/and data confidentiality attacks mentioned in four articles; security misconfiguration mentioned in one study; injection attacks mentioned in three articles; brute force attacks mentioned in one research study; and sensor hijacking attacks mentioned in one article. Other security attacks include cloning attacks mentioned in one paper and denial of service or flooding attacks mentioned in four articles. The chart in figure 5 shows the summaries.

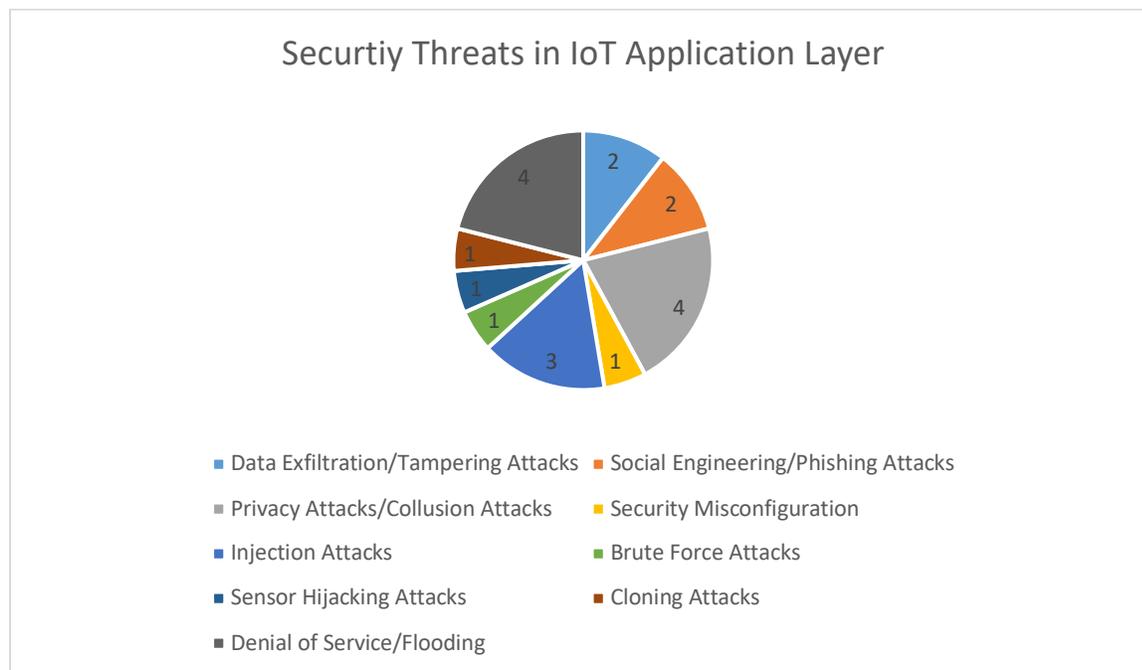


Figure 7: Summary of IoT Application Layer Security Threats

Suitable Countermeasures, Controls, and Solutions

What are the suitable countermeasures, controls, and solutions that healthcare facilities can implement to protect patient health data collected through IoMT, such as wearables and sensor devices, and stored in a cloud environment?

IoT Perception Layer Security Solutions Analysis

Some of the security solutions and countermeasures discovered for threats in the perception layer are summarized in table 9. The solutions are relevant for prioritized and categorized security threats for the IoT perception layer. Based on gathered information on security attacks, various security solutions are recommended, including encryption, gateways, access controls, data anonymization, and privacy-preserving data aggregation.

Table 9: Summary of Solutions to IoT Perception Layer Security Threats

Threat/Attack	Solutions	References
Distributed denial of service attacks (DDoS)/ Denial of sleep attack (DoSL)	Use of encryption (cryptographic algorithms), multi-layer client-server model, gateways.	[40, 53, 54, 57]
Man-in-the-middle attacks/Eavesdropping	Encryption, access control, anonymization of data,	[40, 43, 59]
Physical (local) data tampering attacks	Lightweight and verifiable privacy-preserving data aggregation scheme	[41, 42, 55, 59]
Privacy/Collusion Attacks/Data confidentiality attack/Confidentiality Disclosure/Differential Attacks	BalancePIC – A scheme that attempts to preserve a balance in user privacy, data integrity, and computational cost. Flexible access control with attribute revocation, efficient SIMD homomorphic comparison.	[44-46, 48-52, 54, 55, 58]
False data injection	Encryption and identity-based signature scheme	[47, 54]
Brute force attack and Sybil Attack	Use a 128-bit key sufficient to resist brute force attack Using proxy re-encryption	[56, 60]

IoT Network Layer Security Solutions Analysis

Some of the security solutions and countermeasures discovered for threats in the IoT network layer are summarized in table 10. The selected solutions are based on critical cyber threats in the network layer. After identifying the cyber-attacks targeting the network layer, the following solutions can be deployed to address them. The selected security solutions for the IoT network layer have a risk-based approach with a one-to-one relation with identified security threats.

Table 10: Summary of Solutions to the IoT Network Layer Security Threats

Threat/Attack	Solutions/Countermeasures	References
Hardware misconfiguration	A cryptographic algorithm that prevents unauthorized data access	[40]
Data exfiltration/Tampering attacks/Message attacks	IoT vendors to allow users to authorize client software to access device resources selectively. Random time hopping sequences that detect data tampering in IoMT, formal proof for providing efficiency in data storage and computational services, access control mechanisms based on cryptography, data obfuscation	[41-43, 52, 56, 61, 64, 67, 69]
Denial of service attack	Blockchain technology, using encryption method and authentication method of Ethereum blockchain, identity authentication, and use of anti-DDoS, using hybrid solutions to encrypt IoT communication using Radix-64, a lightweight block cipher Klein.	[62, 64, 70, 71, 75]
Man-in-the-middle attack/ Replay Attack/ Eavesdropping/Reentry attacks	Encryption mechanism (cryptographic algorithms). Wireless body area network (WBAN) security, FGPA authentication, deploying features of blockchain and smart contracts, ensuring complete transaction execution and value transfer before processing the next transaction, use of real-time data streaming model to ensure secure transmission, use a lightweight KATAN secret cipher algorithm in the networked sensor, decentralizing access control	[46, 51, 62, 63, 66, 68, 72]
Brute force attacks/insider keyword guessing	Encryption and outsourced decryption	[65]

Privacy attacks/Collusion attacks/ Code lifting and differential attacks/ Confidentiality disclosure	Putting a threshold on computational costs and IoT devices load, mobile edge computing, white-box cryptography	[44, 45, 48-51]
Injection attack	Enforcing mechanism to deny all access by default, requiring explicit grants, encryption and use of strong passwords	[73]
Spoofing attacks, email compromise	Use of SDN-based data security model based on middlebox-guard (M-G) that aims at reducing network latency	[51, 74]

It is important to consider the IoT application requirements when designing a security solution for IoT devices. For example, (1) battery life is important if the application has hundreds of devices, (2) high-bandwidth is important if the application needs to send lots of data (i.e. video), and (3) time should be considered if the application involves in an automated decision making. Therefore, it's important to develop a security solution based on one of the leading IoT connectivity standards such as LoRa [83], Sigfox [84], and NB-IoT [85].

IoT Application Layer Security Solutions Analysis

Some of the security solutions and countermeasures discovered for threats in the IoT application layer are summarized in table 11. IoT vendors and users face challenges when dealing with increased security controls in the application layer. In this case, they need to prioritize the controls by implementing the most effective ones first. In this research, a risk-based approach is used to prioritize security solutions. The security controls have a direct relation with identified security threats to make them relevant.

Table 11: Summary of Solutions to the IoT Application Layer Security Threats

Threat/Attack	Solutions	References
Data exfiltration/Tampering attacks/Message attacks	Formal proof for providing efficiency in data storage, Using the proposed Mathematical Model for Hybrid Systems for Privacy Preservation,	[42, 76]
Social Engineering attacks/Phishing	Encryption mechanisms to protect communication and sensor data, Multi-layer client-server model that separates virtual and physical gateways, sensors and servers,	[53, 62]

Privacy Attacks/Collusion Attacks/Data confidentiality attack/Differential Attacks	Partial decryption and flexible access control with attribute revocation, Efficient SIMD homomorphic comparison, Public Key Infrastructure (PKI), Aggregation scheme to securely collect data from multiple sources, Trust evaluation, and other pervasive security measures	[43, 45, 46, 48, 56]
Security misconfiguration	Lightweight Privacy-preserving Data Aggregation to filter false data injected by external attackers	[54]
Injection attacks/ Redirects and forwards	SecureData scheme that tackles security issues and avoid following redirects and forwards. Ensure that the supplied value is valid, and authorized for the user, use of blockchain in the IoT platform instead of using MySQL that is prone to attacks	[51, 73, 77]
Brute force attack/Exhaustive search attack	Use of encryption on sensitive data such as user credentials,	[59]
Sensor hijacking attacks	Developing an attack-agnostic way to secure the IoT systems	[78]
Cloning attacks	Forward security, end-to-end security, and key escrow resilience	[79]
Denial of service/Flooding attacks/Botnets/Worm- based attacks	A secure data transmission protocol for low-power IoT devices, with features in Kerberos and one-time password concepts, using cryptographic block and stream ciphers, hashing algorithms, message authentication codes, signature algorithms, and key exchange protocols, scrutinizing network telescope data to report on malicious activities generated by compromised IoT devices	[38, 80-82]
On-off attacks	Using the CWMA to reflect the behavior of the node	[71]



Figure 8: Summary of Popular Security Solutions for IoMT

An analysis of the solutions proposed reveals the increased popularity of encryption in enhancing IoMT security [43, 47, 49, 50, 55-57, 59, 60, 62, 63]. The solution that entails the deployment of conventional and advanced encryption standards work fine in IoT devices, which helps improve security in all the three IoT layers. An analysis of previous studies shows that security-conscious vendors and users should incorporate encryption algorithms in their use of IoT devices in the medical field.

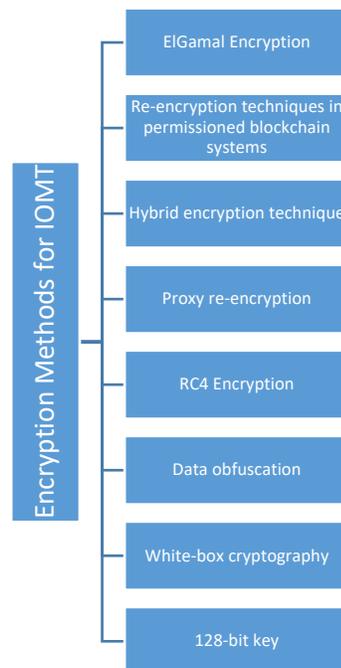


Figure 9: Encryption mechanisms proposed for securing IoMT systems and healthcare data

Apart from encryption, several research studies proposed the use of access control to secure IoMT systems and patients' health data [43, 45, 55, 56, 58, 67, 72, 73]. This security measure involves authenticating and authorizing users to access the information they are only allowed to see and modify in IoMT systems. Various studies proposed different ways to implement access control, as shown in figure 10:

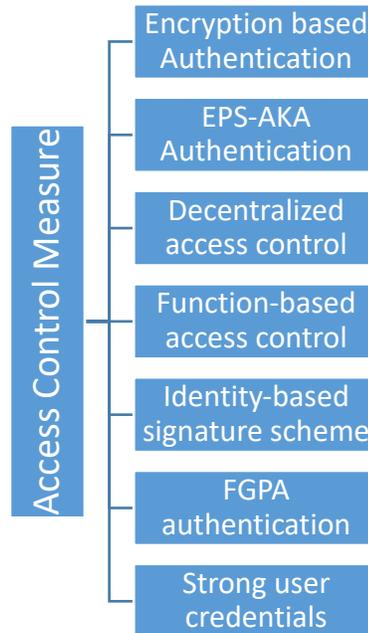


Figure 10: Access control mechanisms used to ensure IoMT Security

An analysis of the study findings also identifies blockchain and smart contracts as an essential security measure in safeguarding IoMT information and systems [57, 58, 66, 74]. For instance, previous studies proposed the use of blockchain technology to contain a denial of sleep attacks that drain the IoMT device's power source, making it malfunction. Other studies recommended the deployment of blockchain and other oracle related techniques to ensure that transactions are entirely executed and the value transfer made before the next transaction is processed [57, 58, 74]. Additionally, users can implement an IoT platform that utilizes blockchain smart contracts on Ethereum to store and manage real-time sensor data in blocks to enhance security.

DDoS is a critical security threat in all layers of the IoT devices and systems. Suo et al. [62] study recommended the use of anti-DDoS protection to prevent denial of service attacks that aim to make IoT services unreachable to authorized users or overwhelm system resources to prevent them from responding to legitimate requests. The proposed mitigation measure analyzes data packets in real-time, diverts incoming traffic, and blocks non-legitimate requests from reaching the server.

Another security method proposed include a secure privacy-protecting aggregation scheme for sensor [48, 49, 51, 55]. This technique provides data integrity and privacy protection and guarantees efficiency in IoT sensor data transmissions and memory use. Real-time data streaming security [65] entails incorporating proper mechanisms to promote efficient and secure transmission of confidential information between IoMT and servers.

Challenges Faced when Securing Health Information in IoMT

What challenges do healthcare institutions face when securing patient health records in a cloud environment and medical IoT devices? As IoMT gains acceptance, companies are implementing security controls and solutions to address risks of loss of patient health information. Successful implementation of IoMT, as discovered in chapter 4, requires an understanding of the security threats involved and the implementation of the security solutions to mitigate frequent and sophisticated cyberattacks.

However, healthcare providers still face challenges when implementing countermeasures to secure healthcare information in IoMT. Table 12 summarizes the challenges faced in IoT perception, network, and application layers.

Challenges faced when Securing IoMT

IoT Perception Layer		IoT Network Layer		IoT Application Layer	
SOLUTIONS	CHALLENGES	SOLUTIONS	CHALLENGES	SOLUTIONS	CHALLENGES
Use of encryption (cryptographic algorithms), multi-layer client-server model, gateways [40, 53, 54, 57]	Businesses need to ensure that a hybrid cryptographic scheme exchange data between nodes securely, challenges of operating big data in complex systems. Requires knowledge of machine learning and data mining	A cryptographic algorithm that prevents unauthorized data access [40, 41]	Requires knowledge of advanced techniques, such as the Diffie-Hellman Key Exchange protocol	Formal proof for providing efficiency in data storage, Using the proposed Mathematical Model for Hybrid Systems for Privacy Preservation [42, 76]	Data aggression is still an issue for data security researchers in IoT cybersecurity. The Big Data size of Healthcare data is a significant problem in Healthcare Information Systems, as well as stringent compliance measures

Encryption, access control, anonymization of data [40, 41, 44]	Conventional encryption algorithms are prone to attacks	IoT vendors to allow users to authorize client software to access device resources selectively. Random time hopping sequences that detect data tampering in IoMT, formal proof for providing efficiency in data storage and computational services, access control mechanisms based on cryptography, data obfuscation [41-43, 52, 56, 61, 64, 67, 69]	Challenges faced while deploying smart meter within an IoT infrastructure. Data aggression in IoT. Additional research on design and deployment of proxy re-encryption	Encryption mechanisms to protect communication and sensor data, Multi-layer client-server model that separates virtual and physical gateways, sensors, and servers [53, 62]	New security and privacy challenges will keep rising as the IoT extends through the traditional Internet that is prone to a wide range of cyber threats. The research needs to be extended to cover future threats to confidentiality and integrity of IoMT. The shortcoming of physical interaction of virtual reflections and real sensors
--	---	---	--	---	--

<p>Lightweight and verifiable privacy-preserving data aggregation scheme [41, 42, 55, 59]</p>	<p>More research is needed on computational cost comparison</p>	<p>Blockchain technology, using encryption method and authentication method of Ethereum blockchain, identity authentication and use of anti-DDoS, using hybrid solutions to encrypt IoT communication using Radix-64, a lightweight block cipher Klein [62, 64, 70, 71, 75]</p>	<p>Intelligent processing is limited for malicious information; there are limitations with existing blockchain models/solutions. The algorithms have different types of structures. The solution only secures communication, leaving the actual IoT system unattended.</p>	<p>Partial decryption and flexible access control with attribute revocation, Efficient SIMD homomorphic comparison, Public Key Infrastructure (PKI), Aggregation scheme to securely collect data from multiple sources, Trust evaluation and other pervasive security measures [43, 45, 46, 48, 56]</p>	<p>It is challenging to address Smart grid application and ensure data security within the IoT network, research, and development of the solutions is still and infancy. It is a challenge to identify when the confidentiality of data in IoT devices is compromised. Proxy re-encryption is a significant challenge as it does not guarantee a solution to altered data</p>
---	---	---	--	---	---

<p>BalancePIC – A scheme that attempts to preserve a balance in user privacy, data integrity, and computational cost. Flexible access control with attribute revocation, efficient SIMD homomorphic comparison [44-46, 48-52, 54, 55, 58]</p>	<p>Effectiveness of cryptography in preserving data confidentiality in IoMT. The concepts of differential privacy and its limitations. Challenges with external encoding invasion, the ciphertext is still prone to attacks</p>	<p>Encryption mechanism (cryptographic algorithms). Wireless body area network (WBAN) security, FGPA authentication, deploying features of blockchain and smart contracts, ensuring complete transaction execution and value transfer before processing the next transaction, use of real-time data streaming model to ensure secure transmission, use a lightweight KATAN secret cipher algorithm in the networked sensor [46, 51, 62, 63, 66, 68, 72]</p>	<p>Requires further testing and improvements Lack of ways to ensure lattice-based cryptography preserves data confidentiality</p>	<p>Lightweight Privacy-preserving Data Aggregation to filter false data injected by external attackers [55]</p>	<p>More research needed on Differential privacy and how it applies within an IoT infrastructure</p>
---	---	---	---	---	---

Encryption and identity-based signature scheme [47, 54]	Increased costs of each computation involved in IoT devices, fog nodes, and the cloud	Encryption and outsourced decryption [67]	Increased computational costs	The SecureData scheme that tackles security issues avoids following redirects and forwards. Ensure that the supplied value is valid, and authorized for the user, use of blockchain in the IoT platform instead of using MySQL that is prone to attacks [51, 73, 77]	The efficiency of hardware-based security. Redirects to central systems may lead to significant data compromise of privacy. Currently, there is no concrete system design and development based on the blockchain
Use a 128-bit key sufficient to resist brute force attack Using proxy re-encryption [56, 60]	Related issues based on data encryption	Putting a threshold on computational costs and IoT devices load, mobile edge computing, white-box cryptography [44, 45, 48-51]	Requires knowledge and further analysis of trust discovery Challenges of ensuring data privacy in mobile edge computing, lack of knowledge in block cipher in IoT, requires expertise in smart grid implementation	Use of encryption on sensitive data such as user credentials [60]	Sophisticated attacks may still bypass poor encryption techniques

Enforcing mechanism to deny all access by default, requiring explicit grants, encryption and use of strong passwords [63]	Attackers using authorized system user can still change URLs or parameters to run a privileged function	Developing an attack-agnostic way to secure the IoT systems [80]	Inability to detect advanced alteration of data in the system
Use of SDN-based data security model based on middlebox-guard (M-G) that aims at reducing network latency [51, 74]	issues of scalability with the proposed model. This solution requires the detailed implementation of the algorithms with various metrics and investigate the protection performance of the algorithms under threats	Forward security, end-to-end security, and key escrow resilience [81]	Requires security with communications between devices to increase network transmission efficiency and reliability

<p>A secure data transmission protocol for low-power IoT devices, with features in Kerberos and one-time password concepts, Using cryptographic block and stream ciphers, hashing algorithms, message authentication codes, signature algorithms, and key exchange protocols, Scrutinizing network telescope data to report on malicious activities generated by compromised IoT devices [38, 80-82]</p>	<p>Limitations of throughput rates An intruder may still interfere with the devices due to its limited functionality, which may cause a massive data breach. Difficulties in investigating the root cause of specific DoS attacks affect mitigation solutions.</p>
<p>Using the CWMA to reflect the behavior of the node [75]</p>	<p>The imperfect monitoring mechanism may compromise the trustworthiness of data</p>

Table 12: Challenges faced when securing IoMT and healthcare information

Summary

This chapter discussed and interpreted the findings in chapter four. The research questions are addressed by analyzing the security threats affecting patient electronic health records in IoMT. The data is analyzed based on the three IoT layers, which include the perception, network, and application layers. The chapter identified key details about security threats, as reviewed in previous research studies. Secondly, the chapter analyzed and categorized the security solutions proposed for mitigating the identified security threats facing IoMT. The chapter also examined the challenges IoMT users face when securing health information.

Chapter 6 : Discussion

Conclusion

The increased connectivity to computer networks in the healthcare sector has become crucial in digital transformation in the industry today. Healthcare service providers deploy devices through the Internet to provide improved and optimized medical care. In effect, users can acquire different wearables that collect, record, and transfer vital health data to the cloud. These devices collect and transmit sensitive electronic health records, prescriptions, medical history, lab results, and patient vitals. Internet of medical things (IoMT) enables physicians with a wide range of benefits and use cases, including monitoring patient health in real-time, implementing and maintaining fitness program, taking care of the elderly, treating chronic diseases remotely, and controlling and sharing patient health data between objects, humans to objects, humans to humans. Different medical devices, such as imaging, sensors, diagnostic equipment, and wearable, form a core part of the IoMT ecosystem.

However, the increased connectivity of the internet of medical things (IoMT) exposes the devices and patient information to cybersecurity threats. The data flow process in the IoMT systems is susceptible to multiple threats since attackers can target numerous entry points, include patient wearables, equipment sensors, and the cloud. Protecting patient IoMT data is vital since it is exposed to various security threats and impacts. Security and privacy of such data are paramount to protecting sensitive information from unauthorized access, breaches, and compromise on confidentiality, integrity, and availability.

This research attempted to discover the security threats affecting patient electronic health records collected and processed through medical wearables and sensor-based IoMT devices and cloud information management. The study identified the pertinent IoT layers threats and shows the way they compromise data privacy and security. Additionally, the research determined suitable countermeasures, controls, and solutions that healthcare facilities can implement to protect patient health data collected through IoMT and stored in a cloud environment. Finally, the research outlined the challenges healthcare institutions face when securing patient health records in a cloud environment and medical IoT devices.

To address these research objectives, the thesis provided an overview of IoMT devices and systems that collect patient information and parameters. The research described the data flow from collection to storage in different stages and identified device constraints. The study outlines a methodology that involved systematically reviewing the literature on IoT data selected through processes

such as data extraction and querying computer science databases. The selected study papers were used to develop the literature review on pertinent IoMT security issues and discuss findings.

The research revealed that IoT systems have a three-layer architecture formed of perception, network, and application layers. The conventional IoT architecture responsible for gathering, processing, and transmitting useful patient information is affected by several security threats, including DDoS, man-in-the-middle attack, eavesdropping, physical data tampering, privacy attacks, false data injection, and brute force attacks at the perception layer. The system's network layer is prone to hardware misconfiguration, data exfiltration and tampering, denial of service attack, man-in-the-middle attack, brute force attack, injection attack, and email spoofing. Finally, the IoT application layer is susceptible to data exfiltration, social engineering (phishing), privacy attacks, security misconfiguration, injection attacks, exhaustive search attacks, sensor hijacking, cloning, flooding attacks, on-off attacks, and worm-based cyber threats.

According to the research, healthcare service providers and other IoMT users can deploy a wide range of countermeasures and controls. IoT perception layer can be secured using encryption, access control, data anonymization, privacy-preserving data aggregation scheme, and proxy-re-encryption. Network layer security controls include cryptography, user access control and authorization, blockchain technology, and installation of anti-DDoS solutions. IoT application layer controls include hybrid systems for privacy preservations, encryption mechanisms, aggregation schemes for securely collecting data from multiple sources, development of an attack-agnostic way to secure IoT systems, key escrow resilience, and deployment of a secure data transmission protocol for low-power IoT devices with features in Kerberos and one-time password concepts.

At the same time, healthcare service providers face challenges when securing health information in IoMT. As IoMT becomes popular in hospitals, stakeholders are implementing a series of security measures to address cyber risks that adversely affect data privacy and life of patients. Unfortunately, such organizations face risks when implementing countermeasures. For instance, IoMT collects massive data, which becomes a challenge to apply stringent security compliance measures. At the same time, threat actors introduce new security and privacy challenges as IoT extend through the conventional Internet prone to numerous vulnerabilities, rendering existing security controls ineffective. Besides, security teams face challenges in real-time identification of security threats in disparate IoT systems and devices located in an extensive area network. One of the recommended security solutions is blockchain technology. However, healthcare service providers lack concrete system design and development based on the blockchain technology. On the other hand, some sophisticated attacks may still bypass poor encryption

techniques used in some IoMT systems. The distributed nature of IoT systems also makes it difficult to investigate the root cause of certain DDoS attacks, which eventually weakens mitigation strategies.

During the study, it was not easy to find the data coherent with the research purpose. Getting different and relevant secondary data sources and peer articles in coherence with this research required ample time and extensive deconstructive reading and analysis to respond to the study objectives. Secondly, summarizing the findings with accurate sources required the development of a connection within the numerous journals. The research involved extensively gathering evidence from the articles and connected its essence with the research's main objective, which was formidable. Time management was critical throughout the process of completing the thesis. Ultimately, this study is crucial for the healthcare sector, medical device manufacturer, clinicians, authorities, and patients seeking to prevent malicious actors from infiltrating IoMT devices and information.

Future Work

Undoubtedly, the explosion of IoT connectivity will remain unmatched in its risk. Smart IoMT devices and systems do not mean secure. With several devices privileged to patient's sensitive data, the prospect of malicious actors infiltrating the intricate cloud of connectivity in the healthcare industry remains a serious threat to the security, privacy, and well-being of patients' data and lives.

Further research should be conducted into ways manufacturers can build IoT devices with security by design mindset. In this case, device vendors begin by selecting a robust and secure operating system that is patchable remotely to mitigate future security vulnerabilities. Meanwhile, as cybercriminals regularly introduce new threats, researchers should recommend flexible and proactive approaches to security, shedding the traditional hardware-centric view of IoT security. Future research should also outline practical strategies healthcare service providers can implement blockchain, a decentralized distributed ledger, to overcome IoMT security challenges. In this case, research should recommend the best way to integrate a blockchain-solution to IoT network, perception, and application layers to solve the numerous privacy and security problems faced with the current model.

References

1. Srinivasan, C., et al., *A review on the different types of Internet of Things (IoT)*. Journal of Advanced Research in Dynamical and Control Systems, 2019. **11**(1): p. 154-158.
2. Dong, P., et al., *Edge computing based healthcare systems: Enabling decentralized health monitoring in Internet of medical Things*. IEEE Network, 2020.
3. Dauwed, M. and A. Meri, *IOT Service Utilisation in Healthcare*, in *IoT and Smart Home Automation*. 2019, IntechOpen.
4. Hindriks, K.V. and J.-J.C. Meyer, *Artificial Intelligence in Health Care and Medicine: A Personalized Approach*. Acta scientific medical sciences, 2019. **3**(10): p. 71-78.
5. Ahamed, F. and F. Farid. *Applying Internet of Things and machine-learning for personalized healthcare: issues and challenges*. in *2018 International Conference on Machine Learning and Data Engineering (iCMLDE)*. 2018. IEEE.
6. Limaye, A. and T. Adegbija. *A workload characterization for the internet of medical things (iomt)*. in *2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 2017. IEEE.
7. Gatouillat, A., et al., *Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine*. IEEE internet of things journal, 2018. **5**(5): p. 3810-3822.
8. Abouzakhar, N.S., A. Jones, and O. Angelopoulou. *Internet of things security: A review of risks and threats to healthcare sector*. in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 2017. IEEE.
9. Sun, W., et al., *Security and privacy in the medical internet of things: a review*. Security and Communication Networks, 2018. **2018**.
10. Hatzivasilis, G., et al. *Review of security and privacy for the Internet of Medical Things (IoMT)*. in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 2019. IEEE.
11. Coventry, L. and D. Branley, *Cybersecurity in healthcare: a narrative review of trends, threats and ways forward*. Maturitas, 2018. **113**: p. 48-52.
12. Oliveira, D., et al., *The Future of Low-End Motes in the Internet of Things: A Prospective Paper*. Electronics, 2020. **9**(1): p. 111.
13. Qureshi, F. and S. Krishnan, *Wearable hardware design for the internet of medical things (IoMT)*. Sensors, 2018. **18**(11): p. 3812.
14. Moosavi, S.R., et al., *End-to-end security scheme for mobility enabled healthcare Internet of Things*. Future Generation Computer Systems, 2016. **64**: p. 108-124.
15. Ullah, F., et al., *Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare*. Sustainable cities and society, 2017. **34**: p. 90-96.
16. Fernandez, A. and K.M. Alexander, *Data Privacy and Confidentiality*. iURBAN: Intelligent Urban Energy Tool, 2016: p. 35.
17. Tounsi, W. and H. Rais, *A survey on technical threat intelligence in the age of sophisticated cyber attacks*. Computers & security, 2018. **72**: p. 212-233.
18. McCusker, K. and S. Gunaydin, *Research using qualitative, quantitative or mixed methods and choice based on the research*. Perfusion, 2015. **30**(7): p. 537-542.
19. Ochieng, P., *An analysis of the strengths and limitation of qualitative and quantitative research paradigms*. Problems of Education in the 21st Century, 2009. **13**: p. 13.
20. Sukamolson, S., *Fundamentals of quantitative research*. Language Institute Chulalongkorn University, 2007. **1**: p. 2-3.
21. Smith, M.L., *Publishing qualitative research*. American educational research journal, 1987. **24**(2): p. 173-183.

22. Fossey, E., et al., *Understanding and evaluating qualitative research*. Australian & New Zealand Journal of Psychiatry, 2002. **36**(6): p. 717-732.
23. Fotheringham, A.S., *Trends in quantitative methods II: stressing the computational*. Progress in Human Geography, 1998. **22**(2): p. 283-292.
24. Gill, P., et al., *Methods of data collection in qualitative research: interviews and focus groups*. British dental journal, 2008. **204**(6): p. 291-295.
25. Aramo-Immonen, H. *Mixed methods research design*. in *World Summit on Knowledge Society*. 2011. Springer.
26. Kitchenham, B. and S. Charters, *Guidelines for performing systematic literature reviews in software engineering*. 2007.
27. Daudt, H.M., C. van Mossel, and S.J. Scott, *Enhancing the scoping study methodology: a large, inter-professional team's experience with Arksey and O'Malley's framework*. BMC medical research methodology, 2013. **13**(1): p. 48.
28. Suresh, P., et al. *A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment*. in *2014 International conference on science engineering and management research (ICSEMR)*. 2014. IEEE.
29. Yang, Z., et al. *Study and application on the architecture and key technologies for IOT*. in *2011 International Conference on Multimedia Technology*. 2011. IEEE.
30. Al Hinai, S. and A.V. Singh. *Internet of things: Architecture, security challenges and solutions*. in *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)*. 2017. IEEE.
31. Qian, Y., et al., *Towards decentralized IoT security enhancement: A blockchain approach*. Computers & Electrical Engineering, 2018. **72**: p. 266-273.
32. Din, I.U., et al., *A decade of Internet of Things: Analysis in the light of healthcare applications*. IEEE Access, 2019. **7**: p. 89967-89979.
33. Corbin, B.A., *When Things Go Wrong: Redefining Liability for the Internet of Medical Things*. SCL Rev., 2019. **71**: p. 1.
34. Johnson, S., *Safeguarding Against Data Breaches*. 2019.
35. Yaqoob, T., H. Abbas, and M. Atiquzzaman, *Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review*. IEEE Communications Surveys & Tutorials, 2019. **21**(4): p. 3723-3768.
36. Mohurle, S. and M. Patil, *A brief study of wannacry threat: Ransomware attack 2017*. International Journal of Advanced Research in Computer Science, 2017. **8**(5).
37. Jalali, M.S. and J.P. Kaiser, *Cybersecurity in hospitals: a systematic, organizational perspective*. Journal of medical Internet research, 2018. **20**(5): p. e10059.
38. Sahu, P., S. Singh, and P. Kumar. *Challenges and Issues in Securing Data Privacy in IoT and Connected Devices*. in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*. 2019. IEEE.
39. Spence, N. and D.P. Paul III, *Ransomware in Healthcare Facilities: A Harbinger of the Future? Perspectives in Health Information Management*, 2018: p. 1-22.
40. Asare, B.T., K. Quist-Aphetsi, and L. Nana. *Secure Data Exchange Between Nodes in IoT Using TwoFish and DHE*. in *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*. 2019. IEEE.
41. Tenório, V., et al. *Low-Cost, Practical Data Confidentiality Support for IoT Data Sources*. in *2019 IX Brazilian Symposium on Computing Systems Engineering (SBESC)*. 2019. IEEE.
42. Zhang, J., et al., *LVPDA: A Lightweight and Verifiable Privacy-Preserving Data Aggregation Scheme for Edge-Enabled IoT*. IEEE Internet of Things Journal, 2020. **7**(5): p. 4016-4027.

43. Karmakar, G.C., R. Das, and J. Kamruzzaman, *IoT Sensor Numerical Data Trust Model Using Temporal Correlation*. IEEE Internet of Things Journal, 2019. **7**(4): p. 2573-2581.
44. Wang, T., et al., *Preserving balance between privacy and data integrity in edge-assisted Internet of Things*. IEEE Internet of Things Journal, 2019. **7**(4): p. 2679-2689.
45. Wu, Y., et al. *Cloud-Supported Internet of Things Data Security and Access Control in Smart Grid*. in *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*. 2019. IEEE.
46. Jiang, L., et al., *Toward Practical Privacy-Preserving Processing Over Encrypted Data in IoT: An Assistive Healthcare Use Case*. IEEE Internet of Things Journal, 2019. **6**(6): p. 10177-10190.
47. Tripathi, A. and S.K. Pasupuleti. *A Secure Lightweight Data Aggregation scheme for Cloud assisted IoT*. in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. 2018. IEEE.
48. Tang, W., et al., *Secure data aggregation of lightweight e-healthcare iot devices with fair incentives*. IEEE Internet of Things Journal, 2019. **6**(5): p. 8714-8726.
49. Saha, A. and C. Srinivasan. *White-Box cryptography based data encryption-decryption scheme for IoT environment*. in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. 2019. IEEE.
50. Li, X., et al., *Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications*. IEEE Internet of Things Journal, 2018. **6**(3): p. 4755-4763.
51. Tao, H., et al., *Secured data collection with hardware-based ciphers for IoT-based healthcare*. IEEE Internet of Things Journal, 2018. **6**(1): p. 410-420.
52. Aman, M.N., et al., *Low power data integrity in IoT systems*. IEEE Internet of Things Journal, 2018. **5**(4): p. 3102-3113.
53. Kakanakov, N. and M. Shopov. *Adaptive models for security and data protection in IoT with Cloud technologies*. in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2017. IEEE.
54. Lu, R., et al., *A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT*. IEEE Access, 2017. **5**: p. 3302-3312.
55. Chaudhry, S. *An Encryption-based Secure Framework for Data Transmission in IoT*. in *2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. 2018. IEEE.
56. Meena, D.K., R. Dwivedi, and S. Shukla. *Preserving patient's privacy using proxy re-encryption in permissioned blockchain*. in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. 2019. IEEE.
57. Muhtasim, M.A., et al. *Secure data transaction and data analysis of IOT devices using blockchain*. in *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*. 2018. IEEE.
58. Cao, J., et al., *Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network*. IEEE Internet of Things Journal, 2018. **6**(2): p. 1561-1575.
59. Abdulrahman, H., N. Poh, and J. Burnett. *Privacy preservation, sharing and collection of patient records using cryptographic techniques for cross-clinical secondary analytics*. in *2014 IEEE Symposium on Computational Intelligence in Healthcare and e-health (CICARE)*. 2014. IEEE.
60. Kumar, M., et al. *Lightweight data security model for IoT applications: a dynamic key approach*. in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 2016. IEEE.
61. D'Orazio, C.J., K.-K.R. Choo, and L.T. Yang, *Data exfiltration from Internet of Things devices: iOS devices as case studies*. IEEE Internet of Things Journal, 2016. **4**(2): p. 524-535.

62. Suo, H., et al. *Security in the internet of things: a review*. in *2012 international conference on computer science and electronics engineering*. 2012. IEEE.
63. Sachdev, H., H. Wimmer, and L. Chen. *Improving Real-Time Data Streaming Security to Promote Patient and Physician Socialization*. in *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)(BDCloud-SocialCom-SustainCom)*. 2016. IEEE.
64. Goel, U., R. Ruhl, and P. Zavorsky. *Using Healthcare Authority and Patient Blockchains to Develop a Tamper-Proof Record Tracking System*. in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. 2019. IEEE.
65. Miao, Y., et al., *Secure online/offline data sharing framework for cloud-assisted industrial internet of things*. IEEE Internet of Things Journal, 2019. **6**(5): p. 8681-8691.
66. Lee, Y.S., E. Alasaarela, and H. Lee. *Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system*. in *The International Conference on Information Networking 2014 (ICOIN2014)*. 2014. IEEE.
67. Khandare, L., D.K. Sreekantha, and K. Sairam. *A Study on Encryption Techniques to Protect the Patient Privacy in Health Care Systems*. in *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*. 2019. IEEE.
68. Al-Asli, M., M.E. Elrabaa, and M. Abu-Amara, *FPGA-Based Symmetric Re-Encryption Scheme to Secure Data Processing for Cloud-Integrated Internet of Things*. IEEE Internet of Things Journal, 2018. **6**(1): p. 446-457.
69. Vijayalakshmi, A.V. and L. Arockiam. *Hybrid security techniques to protect sensitive data in E-healthcare systems*. in *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*. 2018. IEEE.
70. Purohit, K.C., et al. *Hybrid approach for securing IoT communication using authentication and data confidentiality*. in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. 2017. IEEE.
71. Bhattacharjee, S., et al. *Preserving data integrity in iot networks under opportunistic data manipulation*. in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. 2017. IEEE.
72. Al Breiki, H., et al. *Decentralized Access Control for IoT Data Using Blockchain and Trusted Oracles*. in *2019 IEEE International Conference on Industrial Internet (ICII)*. 2019. IEEE.
73. Pankomera, R. and D. van Greunen. *Mitigating vulnerabilities and threats for patient-centric healthcare systems in low income developing countries*. in *2017 IST-Africa Week Conference (IST-Africa)*. 2017. IEEE.
74. Liu, Y., et al., *SDN-based data transfer security for Internet of Things*. IEEE Internet of Things Journal, 2017. **5**(1): p. 257-268.
75. Pallavi, K., V.R. Kumar, and S. Srikrishna. *Comparative Study of Various Lightweight Cryptographic Algorithms for Data Security Between IoT and Cloud*. in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. 2020. IEEE.
76. Kingsford, K.M., et al. *A Mathematical Model for a Hybrid System Framework for Privacy Preservation of Patient Health Records*. in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*. 2017. IEEE.
77. Jeon, J.H., K.-H. Kim, and J.-H. Kim. *Block chain based data security enhanced IoT server platform*. in *2018 International Conference on Information Networking (ICOIN)*. 2018. IEEE.

78. Cai, H., et al. *Deploying data-driven security solutions on resource-constrained wearable IoT systems*. in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*. 2017. IEEE.
79. Fang, D., Y. Qian, and R.Q. Hu, *A Flexible and Efficient Authentication and Secure Data Transmission Scheme for IoT Applications*. *IEEE Internet of Things Journal*, 2020. **7**(4): p. 3474-3484.
80. Lachner, C. and S. Dustdar. *A Performance Evaluation of Data Protection Mechanisms for Resource Constrained IoT Devices*. in *2019 IEEE International Conference on Fog Computing (ICFC)*. 2019. IEEE.
81. Neshenko, N., et al. *Data-Driven Intelligence for Characterizing Internet-scale IoT Exploitations*. in *2018 IEEE Globecom Workshops (GC Wkshps)*. 2018. IEEE.
82. Kurera, C. and D. Navoda. *Node-to-Node Secure Data Transmission Protocol for Low-power IoT Devices*. in *2018 18th International Conference on Advances in ICT for Emerging Regions (ICTer)*. 2018. IEEE.
83. Alliance, L., *The LoRa alliance wide area networks for Internet of Things*. www.lora-alliance.org, 2016.
84. Gomez, C., et al., *A Sigfox energy consumption model*. *Sensors*, 2019. **19**(3): p. 681.
85. Chen, M., et al., *Narrow band internet of things*. *IEEE access*, 2017. **5**: p. 20557-20577.