REPUBLIC OF TÜRKİYE
ALTINBAŞ UNIVERSITY
Institute of Graduate Studies
Information Technologies

SECURING HEALTHCARE IOT DEVICES AND ENABLING SIEM INTEGRATION: ADDRESSING

Mubarak Sa'adu NABUNKARI

Master's Thesis

Supervisor

Asst. Prof. Dr. Muhammad ILYAS

İstanbul, 2024

SECURING HEALTHCARE IOT DEVICES AND ENABLING SIEM INTEGRATION: ADDRESSING

Mubarak Sa'adu NABUNKARI

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY
2024

The thesis titled SECURING HEALTHCARE IOT DEVICES AND ENABLING SIEM INTEGRATION: ADDRESSING prepared by MUBARAK SA'ADU NABUNKARI and submitted on 13/06/2024 has been **accepted unanimously** for the degree of Master of Science in Information Technology.

_____

Asst. Prof. Dr. Muhammad ILYAS

Supervisor

Thesis Defence Committee Members:

Asst. Prof. Dr. Muhammad ILYAS	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	_____
Assoc. Prof. Dr. Jawad RASHEED	Department of Computer Engineering, İstanbul Zaim University	_____

I hereby declare that this thesis meets all format and submission requirements for a Master's thesis.

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Mubarak Sa'adu NABUNKARI

Signature

DEDICATION

I express my gratitude to Almighty Allah for guiding me throughout my education, particularly in completing this final-year thesis project. I appreciate the teachers and lecturers who served as father figures, providing guidance and education. A big thank you to my parents for their unwavering support. Special appreciation to my supervisor for assisting me in the success of the thesis project. I'm also thankful to the administrators of the Information Technology, Department of Computer Engineering, Faculty of Engineering and Architecture and Software Engineering Department for their continuous support during my master's education. Thank you all sincerely.

ACKNOWLEDGEMENT

I want to thank Almighty Allah, the creator of the Universe, for guiding me with His blessings. Our love and respect go to the Holy Prophet Muhammad (P.B.U.H), who has enlightened us through the Holy Quran, guiding us on the path of righteousness and teaching us how to worship Allah (S.A.W) and follow the principles of Islam.

I want to express my eternal gratitude and thanks to God for good health and the gift of life that allowed me to complete this academic journey. I am deeply thankful to everyone who has played a part in making this dissertation possible.

I also wish to express my gratitude to my thesis project advisor, Asst. Prof. Dr. Muhammad Ilyas from Department of Cybersecurity AI Ain University, Abu Dhabi, UAE. He gave me the invaluable chance to work on this thesis project titled " Securing Healthcare IOT Devices and Enabling SIEM Integration: Addressing." His guidance enabled me to conduct meaningful research and acquire new knowledge, and for that, I am sincerely grateful. A special thanks to my parents, siblings, and family who supported me in every situation and prayed for my success.

ABSTRACT

SECURING HEALTHCARE IOT DEVICES AND ENABLING SIEM INTEGRATION: ADDRESSING

NABUNKARI, Mubarak Sa'adu

M.Sc., Information Technologies, Altınbaş University

Supervisor: Asst. Prof. Dr. Muhammad ILYAS

Date: 06/2024

Pages: 52

This thesis explores the growing use of Internet of Things (IoT) devices in healthcare, which has transformed patient care with advanced monitoring and treatment options. However, this integration poses security challenges, demanding robust protective measures. The study focuses on integrating Security Information and Event Management (SIEM) systems with healthcare IoT devices as a solution. Through a thorough literature review, it sheds light on the current state of IoT security, emphasizing the need for improved protective measures. The main issue addressed is the vulnerability of healthcare IoT devices to security breaches and the associated risks to patient data and device functionality. To address this, the research suggests a comprehensive security framework tailored for these devices. This framework, drawn from literature and best practices, includes crucial security measures such as authentication, data encryption, access controls, and anomaly detection. Integrating SIEM systems into this framework provides real-time threat detection and swift incident response, bolstering the overall security of healthcare IoT devices. The thesis highlights the importance of this integration, offering a roadmap for secure, efficient, and effective implementations of healthcare IoT.

Keywords: Cyber Security, Threat Intelligence, Forensics, DDoS Attack, Encryptıon.

ÖZET

SAĞLIK IOT CİHAZLARININ GÜVENLİĞİNİN SAĞLANMASI VE SIEM ENTEGRASYONUNUN SAĞLANMASI: ADRESLEME

NABUNKARI, Mubarak Sa'adu

Yüksek Lisans, Bilişim Teknolojileri, Altınbaş Üniversitesi

Danışman: Dr. Öğr. Üyesi Muhammad ILYAS

Tarih: 06/2024

Sayfa: 52

Bu tez, gelişmiş izleme ve tedavi seçenekleriyle hasta bakımını dönüştüren Nesnelerin İnterneti (IoT) cihazlarının sağlık hizmetlerinde artan kullanımını araştırıyor. Ancak bu entegrasyon, güçlü koruyucu önlemler gerektiren güvenlik zorlukları doğurmaktadır. Çalışma, bir çözüm olarak Güvenlik Bilgi ve Olay Yönetimi (SIEM) sistemlerini sağlık hizmeti IoT cihazlarıyla entegre etmeye odaklanıyor. Kapsamlı bir literatür taraması yoluyla, iyileştirilmiş koruyucu önlemlere olan ihtiyacı vurgulayarak IoT güvenliğinin mevcut durumuna ışık tutuyor. Ele alınan ana konu, sağlık hizmeti IoT cihazlarının güvenlik ihlallerine karşı savunmasızlığı ve hasta verileri ve cihaz işlevselliğine yönelik ilgili risklerdir. Bu konuyu ele almak için araştırma, bu cihazlara özel olarak tasarlanmış kapsamlı bir güvenlik çerçevesi önermektedir. Literatürden ve en iyi uygulamalardan alınan bu çerçeve, kimlik doğrulama, veri şifreleme, erişim kontrolleri ve anormallik tespiti gibi önemli güvenlik önlemlerini içerir. SIEM sistemlerinin bu çerçeveye entegre edilmesi, gerçek zamanlı tehdit tespiti ve hızlı olay müdahalesi sağlayarak sağlık hizmetleri IoT cihazlarının genel güvenliğini artırır. Tez, sağlık hizmetlerinde IoT'nin güvenli, verimli ve etkili uygulamaları için bir yol haritası sunarak bu entegrasyonun önemini vurgulamaktadır.

Anahtar Kelimeler: Siber Güvenlik, Tehdit İstihbaratı, Adli Tıp, DDoS Saldırısı, Şifreleme.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVATIONS

ATT&CK	:	Adversarial Tactics, Techniques, and Common Knowledge
DLP	:	Data Loss Prevention (DLP)
EDR	:	Endpoint Detection and Response (EDR)
FDA	:	Food and Drug Administration
HC3	:	Health Sector Cybersecurity Coordination Centre
HE	:	Homomorphic Encryption
HHS	:	Department of Health and Human Services
HICP	:	Health Industry Cybersecurity Practices
HPH	:	Health and Public Health
IDS	:	Intrusion Detection System
IEC	:	International Electrotechnical Commission
IoT	:	Internet of Things (IoT)
IPS	:	Intrusion Prevention System (IPS)
ISMS	:	Information Security Management Systems
ISO	:	International Organization for Standardization
MFA	:	Multi-Factor Authentication (MFA)
MITRE	:	MITRE Corporation
NIST	:	National Institute of Standards and Technology
p-PUF	:	Photonic Physical Unclonable Functions
SIEM	:	Security Information and Event Management (SIEM)
SP	:	Special Publication
SPSOS	:	Smart Open Service for European Patients
TEE	:	Trust Execution Environment

1. INTRODUCTION

In our fast-changing world, the Internet of Things (IoT) has introduced a new era of connectivity, where everyday objects communicate seamlessly, transforming various aspects of our lives. The IoT creates a space where devices, from household items to personal gadgets, can share information without human intervention. This interconnected system has particularly impacted healthcare, bringing about significant changes in patient care and operational efficiency. IoT devices play a crucial role in reshaping healthcare practices by facilitating data exchange and real-time insights across geographical boundaries. This connectivity has improved patient care, remote monitoring, and overall health outcomes [8, 31].

For instance, IoT is used in remote patient monitoring, allowing continuous tracking of vital signs like heart rate, blood pressure, and glucose levels. Healthcare providers can monitor patients in real-time, providing timely interventions during emergencies [5]. Moreover, the integration of IoT in healthcare has given rise to intelligent medical devices such as insulin pumps and wearable health trackers. These devices collect real-time data, enabling personalized treatment plans for optimal patient outcomes while reducing the need for frequent healthcare visits. This technological collaboration also extends to telemedicine, enabling virtual consultations to address gaps in access to medical expertise, especially in remote areas [8, 21].

The Internet of Things (IoT) plays a vital role in managing medications by sending timely reminders to patients and caregivers, ensuring adherence. In hospitals, IoT solutions enhance efficiency by tracking medical equipment and assets. The data generated by IoT enables real-time healthcare analytics, supporting informed decisions and a data-driven approach to patient care. IoT also contributes to infection control and environmental monitoring in hospitals, maintaining hygiene standards and patient safety [24, 32]

In the realm of ambient assisted living, IoT-based home monitoring systems empower elderly and disabled individuals, promoting independence while ensuring timely assistance. This research envisions a solution that combines IoT and machine learning (ML) to address challenges posed by the COVID-19 pandemic [25, 33]. By continuously monitoring patients' health using IoT, vital biological data is extracted and analysed with ML algorithms to assess

the severity of the virus. This enhances remote patient monitoring, allowing for prompt medical interventions while minimizing the risk of viral transmission.

However, the increasing connectivity of healthcare IoT raises cybersecurity concerns. The vulnerabilities created by this interconnectedness can be exploited by cyberattacks, posing risks to patient well-being and sensitive data. The research emphasizes the urgent need for robust cybersecurity measures to ensure patient safety and maintain data confidentiality.

This research tackles the urgent issue of improving security for healthcare IoT by incorporating Security Information and Event Management (SIEM) systems. The study involves a thorough examination of existing SIEM solutions for healthcare, revealing that many current solutions don't fully address the structural aspects of IoT, as confirmed by the literature review. The integration of SIEM aims to overcome the specific security challenges posed by healthcare IoT devices, ensuring the safety of patients and the protection of sensitive data. The research objectives include identifying IoT security challenges, exploring the potential of SIEM integration, suggesting a comprehensive security framework, and assessing the framework's effectiveness using MITRE ATT&CK standards. In summary, combining healthcare IoT with SIEM marks a shift in fundamental assumptions, reshaping patient care, remote monitoring, and operational efficiency.

1.1 BACKGROUND

The integration of Internet of Things (IoT) devices in healthcare has brought about significant changes, enabling real-time monitoring of patients, telemedicine, and remote care [5]. However, this integration has also introduced security challenges, particularly due to the sensitive nature of health data and the potential consequences of a security breach [28]. In response to these challenges, Security Information and Event Management (SIEM) systems have been developed and put into use. These systems allow for the real-time analysis of security alerts generated by applications and network hardware [26].

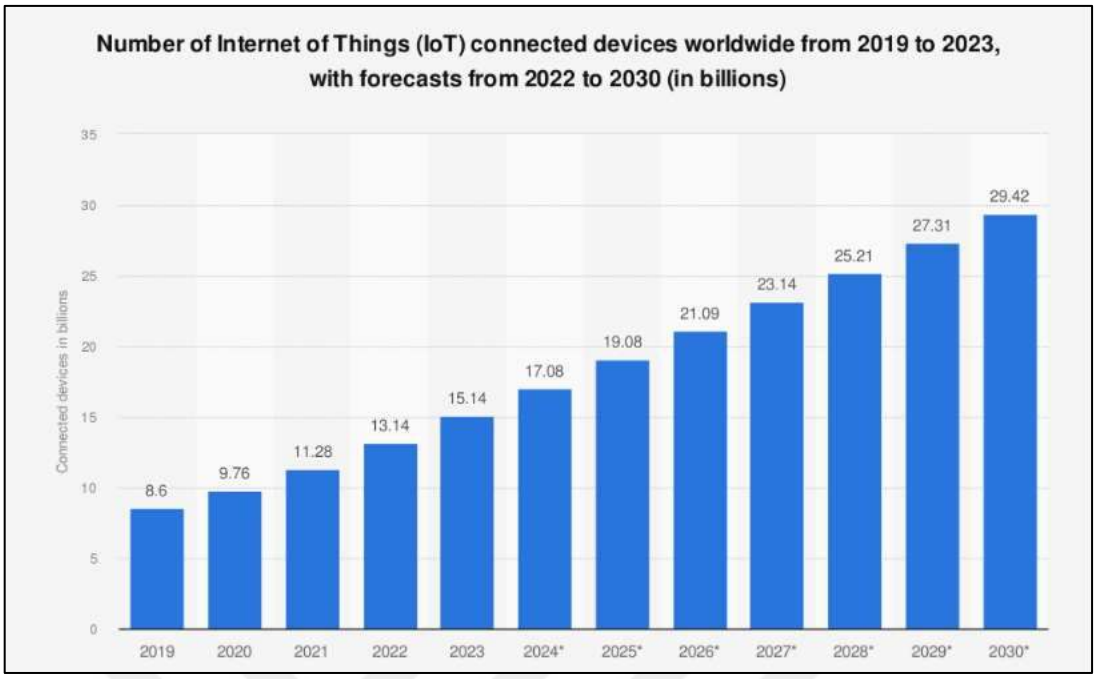

Figure 1.1: Displays Statistics and Future Forecasts For The Internet Of Things (IoT), Sourced From Statista In 2023.

In 2023, the healthcare sector faced a major threat from cyberattacks, particularly affecting IoT devices. Statista estimated that the number of IoT devices in healthcare would increase to 35.82 million by 2023, up from 28.27 million in 2021 [13]. However, this growth coincided with a sharp rise in cyberattacks. According to Insider Intelligence, global healthcare organizations experienced an average of 1,463 cyberattacks per week in 2022, a 74% increase from 2021. In the U.S., healthcare entities faced an average of 1,410 weekly cyberattacks per organization, marking an 86% increase from the previous year (Benbya et al 2020). IoT attacks constituted a significant part of this threat landscape, with 53% of connected devices at risk of a cybersecurity attack. IV pumps, representing 38% of a hospital's IoT devices, and VoIP systems, making up 50%, were identified as the most vulnerable [16].

In the United Kingdom, both the government and the National Health Service (NHS, 2023) actively engage in integrating and securing IoT devices in healthcare. The NHS employs IoT for tracking valuable resources and equipment. The UK government has issued a Code of Practice for Consumer IoT Security, outlining thirteen guidelines for good practice in IoT security. NHS Digital offers cybersecurity guidance for healthcare professionals dealing with Connected Medical Devices (CMDs). Furthermore, strategic partnerships have been formed to enhance IoT security in the UK healthcare market. For instance, Cynerio and

Integra e-Quip teamed up to address security needs on the Internet of Medical Things (IoMT). Similarly, Cynerio and IT Health joined forces to enhance visibility and security for IT, IoT, and medical device infrastructure in NHS organizations. The global IoT in healthcare market, valued at USD 252.1 billion in 2022, is expected to grow at a compound annual growth rate (CAGR) of 16.8% between 2023 and 2030, according to recent statistics [18, 35]

Hospitals, clinics, nursing homes, and even patients' homes are beginning to use IoT devices in healthcare. Wearables like fitness trackers and smartwatches are commonly used, allowing patients to monitor their fitness and health conditions in real-time [35]. Despite the benefits of IoT in healthcare, including remote medical assistance and real-time tracking, there are significant challenges. One major concern is data protection and privacy maintenance. Many IoT devices lack established data guidelines and security standards, raising uncertainty about data ownership. This uncertainty makes the data vulnerable to hackers who could breach the system and compromise the confidential health information of both medical practitioners and patients [16]. These challenges highlight the urgent need for strong cybersecurity measures in the healthcare sector, especially for IoT devices. Regarding the security of healthcare IoT devices and the integration of Security Information and Event Management (SIEM), the paper proposes that dynamic risk assessment methods can offer a more effective and real-time approach to identifying and addressing potential security risks. This could enhance SIEM systems by providing them with more timely and accurate information about potential security threats [21]. Various companies have developed SIEM solutions, including IBM's QRadar SIEM and Splunk's Enterprise Security solution.

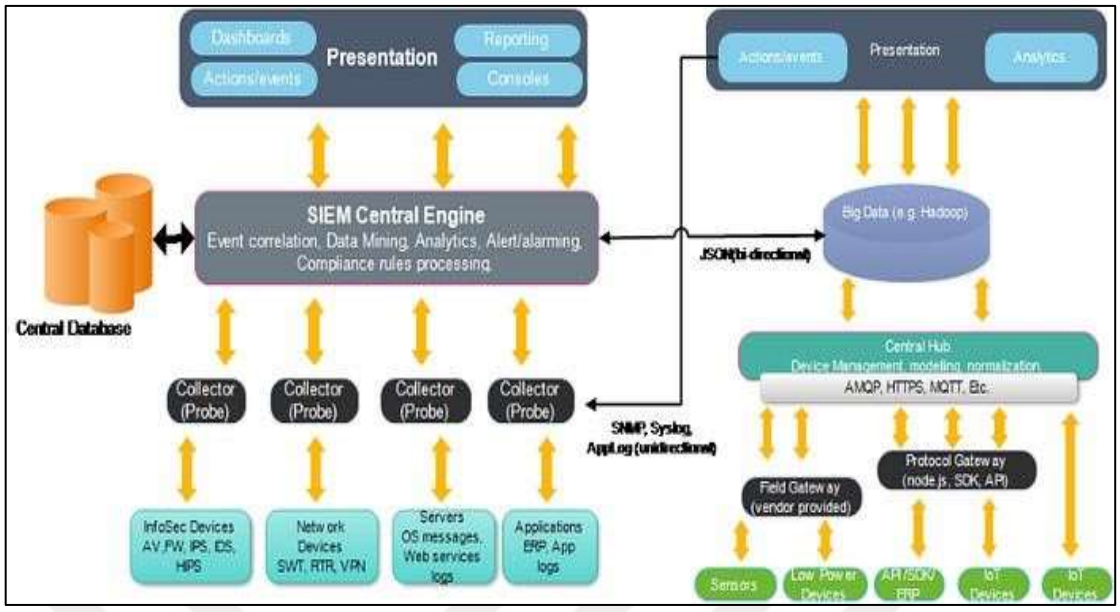

Figure 1.2: Shows the Integration of Internet of Things (IoT) and Security Information and Event Management (SIEM), as Sourced from Tembe in 2018.

SIEM systems are now used in healthcare to secure IoT devices, monitor network activity, and respond to security threats in real-time. They have proven effective in identifying and responding to threats, enhancing the security of Healthcare IoT to some extent, as shown in the literature study. Although there have been significant advancements in using SIEM systems to secure IoT devices in healthcare, ongoing research is necessary. Despite these systems' effectiveness, cyberattacks on healthcare IoT devices persist, emphasizing the need for continuous research and development to improve the efficiency of SIEM systems and other security solutions [24].

The integration of IoT devices into healthcare systems brings many benefits but also significant challenges, especially in terms of data security and privacy. The use of SIEM systems holds promise in addressing these challenges, but further research and development are required to enhance their effectiveness and tackle the unique security issues posed by IoT devices in healthcare. This research aims to conclude with a framework that covers the security and improvement gaps.

1.2 MOTIVATION

This research is motivated by the pressing need to address security issues concerning healthcare IoT devices and the integration of Security Information and Event Management (SIEM) systems in the UK. The increasing reliance on IoT devices for personalized patient

care in the UK healthcare sector has raised significant security concerns. The growing use of these devices poses potential safety risks for patients and jeopardizes the confidentiality of healthcare data. The interconnected nature of healthcare IoT makes it an attractive target for cybercriminals seeking unauthorized access and manipulation. Such breaches could lead to adverse patient outcomes, a decline in trust, and financial consequences. The NHS in the UK, a prominent healthcare service provider, acknowledges the importance of robust cybersecurity measures to safeguard patient well-being (NHS, 2023). The rising number of sophisticated cyberattacks on healthcare institutions in the UK highlights the need for effective defensive strategies. Understanding the tactics used by attackers is essential for developing strong security protocols. The integration of healthcare IoT with SIEM provides centralized monitoring, event correlation, and real-time threat detection, enabling proactive detection and response [25]. This research aims to offer practical recommendations to enhance cybersecurity, ensure patient safety, and protect data privacy within the UK.

1.3 PROBLEM STATEMENTS

Recently, the healthcare industry has enthusiastically adopted IoT devices, such as medical wearables and interconnected medical equipment, to improve patient care and streamline operations. However, as these devices become more connected, they encounter new security challenges. Cyberattacks can target healthcare IoT devices, endangering patient safety and sensitive medical data. It is crucial to establish robust cybersecurity measures to safeguard patients and ensure the security of their medical information. This consideration played a vital role in shaping the key questions for this research study.

1.4 RESEARCH QUESTIONS

This study will use the gathered and analysed data to address the following questions, which have been further broken down into specific aims and objectives:

a. What are the potential advantages and drawbacks of combining SIEM systems with healthcare IoT devices, and how can SIEM capabilities be utilized to enhance the identification and response to security incidents in healthcare IoT environments?
b. How can we create a comprehensive security framework for healthcare IoT devices that tackles recognized security issues, incorporates best practices, and includes crucial

security measures like authentication methods, data encryption, access controls, and anomaly detection?

c. What is the impact of implementing the proposed security framework on improving the overall security status of healthcare IoT devices, including the accuracy of threat detection and the time it takes to respond to incidents when applied in real-world healthcare settings?

1.5 AIM AND OBJECTIVES

1.5.1 Aim

This research aims to make healthcare IoT devices more secure by integrating them effectively with SIEM systems. The focus is on tackling the specific security issues faced by healthcare IoT devices and using the capabilities of SIEM to enhance the overall cybersecurity of healthcare organizations, safeguarding patient safety and confidential data.

1.5.2 Objectives

a. Find out problems with security in healthcare IoT and check the current SIEM.
b. Explore how SIEM can be used in healthcare IoT settings.
c. Suggest a complete security plan for healthcare IoT devices.
d. Test how well the suggested plan works using MITRE ATT&CK.

1.6 DISSERTATION STRUCTURE

Figure 3 shows the start of the research topic and its goals. It goes on to include a review of existing literature, the proposed framework, analysis and standardization, discussion of future work and recommendations, and finally, a conclusion that summarizes the entire study. This structure gives a clear idea of how the dissertation is organized.

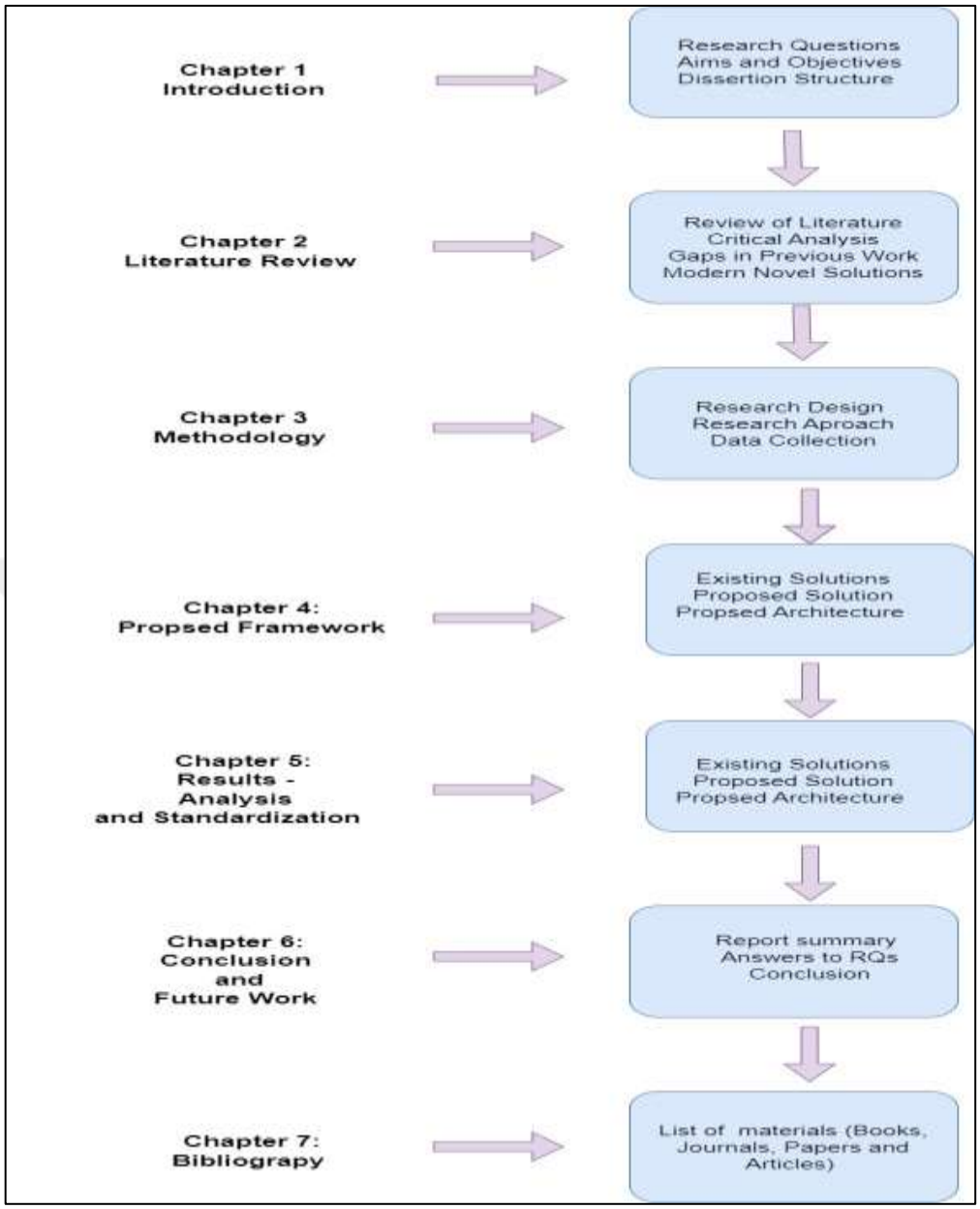

Figure 1.3: Dissertation Structure.

2. LITERATURE REVIEW

Many studies and research have investigated the security problems of healthcare IoT devices and combining them with SIEM. This part reviews what others have already studied and researched in this area. It points out the methods, frameworks, and solutions suggested by researchers and industry experts.

2.1 REVIEW OF EXISTING LITERATURE

In a study [23], they pointed out that interconnected devices, like those in healthcare IoT, are at risk of security problems and privacy issues. They highlighted that vulnerabilities in these devices can let attackers steal important patient data. They specifically mentioned Denial-of-Service (DoS) attacks as a significant threat to IoT devices, which happens because of limitations like bandwidth and memory. To address this, they suggested using a security system called SIEM, which can efficiently monitor and block malicious content in data packets. They also suggested improving SIEM by using learning for real-time detection and exploring new ways to make IoT devices more secure.

Another study by Chacko and Hayajneh in 2018 discussed the advantages and challenges of bringing IoT into healthcare, especially for patient monitoring and data analytics. They noticed that the security risks of connecting these devices to the internet were not given enough attention. They explored the role of IoT in healthcare, its vulnerabilities, security problems, and solutions. They also mentioned the FDA's guidance on handling cyber vulnerabilities in medical devices. The researchers brought attention to potential attacks on devices like pacemakers and predicted ransomware threats for medical devices. They stressed the importance of having enforceable security policies, doing vulnerability assessments, and monitoring events to protect against possible cyber threats.

In a study by Lopez and team in 2018, they introduced a wireless system that can detect and report harmful activities to a security system called SIEM, safeguarding IoT devices from cyber-attacks. They did many experiments to show that their system works well in typical IoT environments. They also suggested doing more research on collaborative detection, how the SIEM system reacts to alerts, and testing intrusion detection on other wireless technologies like Bluetooth or Zigbee, which are used in medical devices.

Adat and Gupta in 2018 focused on challenges in Europe regarding the privacy and security of health data when shared between EU countries. They talked about two projects, SPSOS and KONFIDO, which use advanced technologies like homomorphic encryption, photonic Physical Unclonable Functions (p-PUF), SIEM systems, and blockchain-based auditing to make cross-border health data exchange more secure. They suggested using these technologies for a safe global exchange of health data.

[38] dealt with security challenges in big data analytics in healthcare. They proposed a solution called CIMVHR Data Safe Haven (CDSH) along with a SIEM system to detect intrusions better. They aimed to enhance encryption methods for continuous monitoring and updating security protocols to fully use big data analytics while keeping patient data secure.

Pantelis and others in 2021 presented a method to secure important healthcare processes using modern technologies for accurate risk assessment. They suggested using the KONFIDO project technology and the SIEM tool along with Homomorphic Encryption (HE) and Trust Execution Environment (TEE) to improve privacy and integrity. They tested their approach in Smart Hospitals, ensuring high-security standards and using cost-effective and open-source products that could be applied to different-sized medical devices. They validated their method using real cases from European public hospitals.

In a study by Boca and team in 2023, they suggested, planned, and studied a complex IoT system for higher education, where IoT devices monitor data. Even though their research wasn't about healthcare, it could give useful ideas about modelling and analysing IoT systems that might be helpful in healthcare.

Singh and colleagues in 2023 created medical devices with health sensors and used blockchain to store and check patient information in their suggested system. Their focus was on using IoT and Blockchain together as a secure platform to deal with the shortage of nurses, a big problem in healthcare.

Ylönen, and team in 2020 investigated the latest research on smart wearable devices, especially analysing the challenges of making sure IoT-based drug delivery systems are safe and effective in healthcare. This is important because wearable devices for monitoring and treatment are becoming more common in healthcare.

Czekster and others in 2023 did a detailed review of how to assess risks in Medical Internet-of-Things (MIoT), looking at current trends and existing methods. They found important ways to lessen the impact of unauthorized access and protect users from personal data leaks,

ensuring that devices work without interruption. This is crucial because in healthcare, the security of patient data and the proper functioning of devices are extremely important.

2.2 SIEM SOLUTIONS

To figure out what Security Information and Event Management (SIEM) options are there for healthcare providers, we looked at the top 5 SIEM solutions. Table 1 shows a brief overview of their features, descriptions, differences, and any areas where they might be lacking.

Table 2.1: Lists SIEM Solutions That Healthcare Providers Can Use.

SIEM Solution	Features	Description	Distinctions	Gaps
Splunk (Splunk, 2023)	Collecting data in real-time, using machine learning, advanced analytics, threat intelligence, and analysing user behaviour.	Splunk is a platform that helps search, monitor, and investigate large amounts of data generated by machines. It uses machine learning and advanced analytics to find and respond to threats in real-time.	Splunk is famous for its smart analysis and machine learning features that make it good at finding unknown threats and minimizing false alarms.	Although Splunk provides sophisticated analytics and threat intelligence customized for the healthcare industry, it doesn't specifically offer a complete security framework specifically designed for healthcare IoT devices (Splunk, 2023).

Table 2.1: Lists SIEM Solutions That Healthcare Providers Can Use “Table Continued”.

ArcSight (Focus, 2023)	Instant event connection, recognizing threats as they happen, understanding user behaviour, and managing logs.	ArcSight is a cybersecurity tool that spots and reacts to security incidents by connecting events in real-time, managing logs, and offering threat intelligence.	ArcSight is recognized for its ability to quickly connect events as they happen, making it effective in identifying intricate attack patterns throughout the network.	ArcSight doesn't offer a complete security plan specifically designed for healthcare IoT devices, and its effectiveness isn't aligned with MITRE ATT&CK.
LogRhythm (LogRhythm, 2023)	Advanced SIEM, Analysing User and Entity Behaviour, Examining Network Traffic Patterns, and Utilizing Security Automation and Orchestration	LogRhythm, as a NextGen SIEM platform, brings together User and Entity Behaviour Analytics (UEBA), Network Traffic and Behaviour Analytics (NTBA), and Security Automation and Orchestration (SAO) to identify and address threats immediately.	LogRhythm is recognized for its ability to automate security actions and coordinate them efficiently, contributing to streamlined security operations.	LogRhythm doesn't offer a detailed security plan tailored for healthcare IoT devices and doesn't demonstrate its effectiveness in this specific context.

Table 2.1: Lists SIEM Solutions That Healthcare Providers Can Use "Table Continued".

				onto MITRE ATT&CK.
IBM (IBM, 2023)	Instant analysis of data, understanding potential threats, managing logs, Analysing network traffic.	IBM QRadar is a security solution that uses real-time analysis, threat information, and examining network traffic to identify and address security issues.	IBM QRadar is recognized for its ability to analyse network traffic, aiding in the identification of potentially harmful activities on the network.	IBM QRadar does not have a complete security plan designed specifically for healthcare IoT devices and doesn't demonstrate its effectiveness against MITRE ATT&CK.
SolarWinds (SolarWinds, 2023)	Log and event management, Compliance reporting, Real-time event correlation, User activity monitoring	SolarWinds is a security solution that helps manage logs and events, generate compliance reports, and correlate real-time events to identify and respond to security incidents.	SolarWinds is recognized for its ability to generate reports that ensure organizations meet regulatory requirements.	SolarWinds lacks a specialized security framework for healthcare IoT devices and does not demonstrate its effectiveness according to MITRE ATT&CK.

2.3 CRITICAL ANALYSIS OF THE LITERATURE

The information from the reviewed studies shows a few important things:

a. IoT Devices Security Risks: Many researchers agree that healthcare IoT devices, like glucose meters and pacemakers, can be attacked in different ways, such as DDOS, malware, med jacking, and ransomware threats [19, 23]
b. SIEM Integration: Some studies suggest combining SIEM systems with other technologies like Intrusion Detection Systems (IDS), Homomorphic Encryption (HE), and Trust Execution Environment (TEE) to make healthcare IoT devices more secure and private [30].

c. Cross-Border Data Exchange: Sharing health data between different places is tricky because of privacy and security worries. New technologies like homomorphic encryption, photonic Physical Unclonable Functions (p-PUF), and blockchain-based auditing are suggested to make cross-border health data exchange more secure [36].
d. Big Data Analytics: Handling big data in healthcare has security challenges, like protecting data storage and ensuring patient privacy. Some solutions proposed include using CIMVHR Data Safe Haven (CDSH) and SIEM systems for better intrusion detection, and regularly updating security protocols [38].
e. Wireless Communication: Since most IoT devices communicate wirelessly, there's a risk of eavesdropping attacks. Solutions suggested including using Intrusion Detection Systems (IDS) with SIEM and exploring collaborative scenarios for better detection and reactions from the SIEM system.

2.3.1 Denial-of-Service (DOS) Attacks

IoT devices and apps are easily attacked by something called DoS because they don't have a lot of resources like enough internet speed, memory, or power. One way to deal with this is to use SIEM systems, which can stop bad stuff by carefully watching the information packets and quickly figuring out if something is wrong. This was suggested by Eken and Eken in 2018, and Yang and others in 2023 also agree.

2.4 ANALYSIS OF STUDIES FROM 2023

The new studies from 2023 support what we learned before and bring in some new ideas and solutions to handle security problems with IoT devices in healthcare. Here are the main points:

a. IoT System Modelling and Analysis: Boca and team in 2023 suggested, planned, and studied a complicated IoT system for higher education. Even though it wasn't about healthcare, it might give us useful ideas about modelling and analysing IoT systems that could help in healthcare.
b. Blockchain Integration: Singh and others in 2023 made medical gadgets with health sensors and used blockchain to store and check patient information. They focused on

combining IoT and Blockchain to make a secure system and deal with the shortage of nurses.

c. Smart Wearable Devices: Raikar and team in 2023 investigated the newest research on smart wearable devices, especially focusing on the challenges of making sure IoT-based drug Table 2 gives a summary of the important things we found, and the ideas suggested in the reviewed studies. It shows the different security problems that IoT devices in healthcare might have and the creative ways researchers have suggested to deal with these issues.

d. delivery systems are safe and effective in healthcare.

e. Dynamic Risk Assessment: Czekster and colleagues in 2023 did a detailed review of how to assess risks in Medical Internet-of-Things (MIoT), looking at current trends and existing methods. They found important ways to lessen the impact of unauthorized access and protect users from personal data leaks, making sure devices work without interruption.

2.5 SUMMARY OF LITERATURE RESULTS

We can find summary of literature results in Table 2.2.

Table 2.2: Provides a Summary of The Literature Review.

Author(s)	**Year**	**Key Findings**	**Proposed Solutions**
Eken & Eken	2016	IoT devices and applications are especially at risk of experiencing Denial of Service (DoS) attacks.	SIEM-based systems are employed to efficiently monitor data packets and use learning for real-time detection to block malicious content.
Chacko & Hayajneh	2018	Not taking security risks into account when connecting healthcare IoT devices to the internet.	Establish and follow security rules, check for weaknesses, and keep an eye on events that may pose a threat.
Nespoli & Gómez Mármol	2018	Wireless communication among IoT devices can be at risk of eavesdropping attacks.	Utilizing IDS architecture alongside SIEM and exploring collaborative scenarios for detection and SIEM server responses to received alerts.

Table 2.2: Provides a Summary of The Literature Review "Table Continued".

Al-Yang, & Wu, 2023	2020	Weaknesses in IoT devices provide attackers with an entry point to pilfer sensitive patient information.	Improve SIEM by using learning for detecting issues in real-time and find new ways to make IoT devices more secure and safe from big disruptions.
Rakha	2022	Difficulties with keeping healthcare data safe when using big data analytics.	We use CIMVHR Data Safe Haven (CDSH) and SIEM systems to improve spotting intruders and to always keep an eye on security by regularly updating protocols.
Zaman et al	2022	It's important to use the latest technologies to accurately assess risks in healthcare procedures.	We use technology from the KONFIDO project, a SIEM tool, Homomorphic Encryption (HE), and Trust Execution Environment (TEE).
Sharma & Aujla	2023	Problems arise when sharing health data across borders because of worries about privacy and security.	We use advanced technologies like homomorphic encryption, photonic Physical Unclonable Functions (p-PUF), and auditing with blockchain.
Singh et al.	2023	There is a need for a safe platform to help address the shortage of nurses.	Creating medical devices that use healthcare sensors and utilize blockchain to store and confirm patient information.

2.6 KEY GAPS IDENTIFIED

In the studies we looked at and what I'm going to cover in this dissertation, we found some important gaps:

a. Not Enough Healthcare Solutions: Even though many studies suggest ways to solve specific security problems, there's a lack of complete solutions that deal with multiple security challenges at once, especially for healthcare. Table 2 shows this. While there are some solutions, there are still gaps that need more work in this area.
b. Not Enough Focus on IoT Integration: A lot of the suggested solutions give services for SIEM in things like Cloud and other technologies, according to our analysis of previous

work. This leaves a gap for more work and a framework, especially when it comes to IoT.

c. Need for Standardization: The solutions suggested don't follow a standard way of doing things, making it hard to use them in different healthcare systems and with different devices. We need to set standards, like following NIST and MITRE ATT&CK, to make things more organized and consistent.

3. METHODOLOGY

The fast progress of the Internet of Things (IoT) has changed healthcare, allowing for real-time monitoring of patients, data analysis, and automation of various tasks. However, the increase in IoT devices has also brought up serious worries about security. Making sure these devices are secure is very important to protect important patient information and keep healthcare services running smoothly. This dissertation plans to suggest a complete system to make IoT devices in healthcare more secure. It will check how well this system works using online standards like NIST, ISO, and MITRE ATT&CK. To do this, the research will use a qualitative method, which means it will rely on existing data to support the suggested system. This method was picked because it lets us carefully look at existing studies, systems, and standards, making it easier to suggest a new and stronger system. This chapter explains how this dissertation will be done, including the research approach, collecting data, criteria, analysis methods, ethical concerns, and any limits to the study.

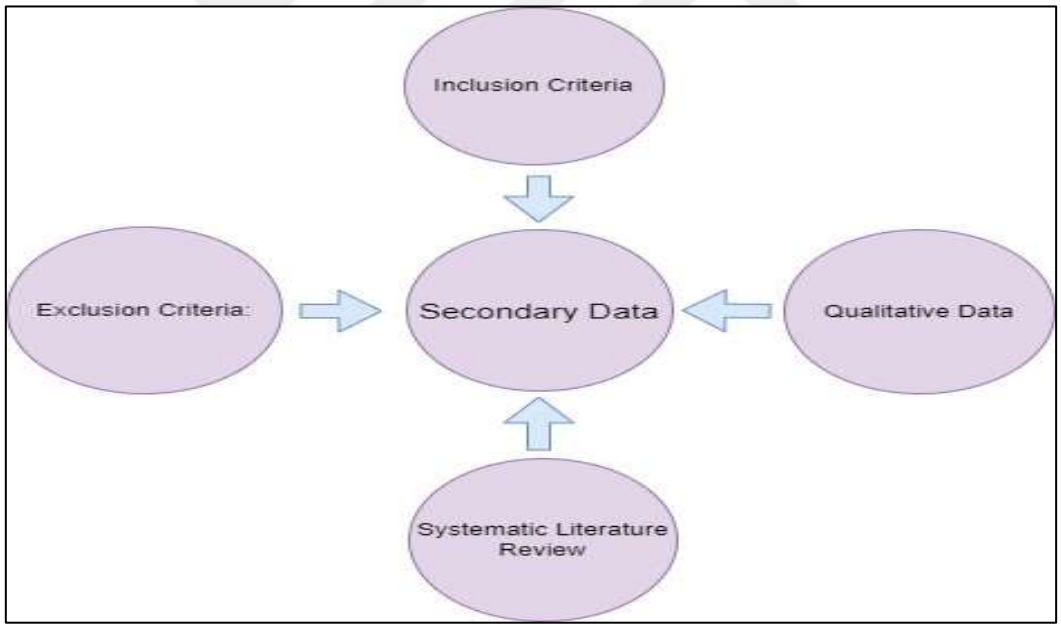

Figure 3.1: Gives an Overview of The Methodology.

3.1 RESEARCH APPROACH AND DESIGN

This research is based on a way of doing things called qualitative methodology because it's the best fit for understanding the complexities of IoT security in healthcare. In this approach, we collect and look at non-number data like text to understand ideas, opinions, or

experiences. For this research, we're going to do a detailed review and analysis of existing studies, systems, and standards related to security for IoT in healthcare.

3.2 APPROACH

We picked the qualitative approach for a few reasons. Firstly, it helps us really understand how secure IoT is in healthcare by looking at existing studies and systems. Secondly, it lets us find out what's missing or not working well in current approaches, which is important to suggest a better system. Lastly, it helps us check if the suggested framework works well by comparing it to established standards like NIST and ISO, making sure it's strong and useful in real-life situations.

3.3 DESIGN

The research plan includes three main steps:

a. Reading Existing Studies: We will carefully read existing studies on IoT security in healthcare, including academic articles, reports, and current frameworks and standards. The goal is to learn how secure IoT is in healthcare right now, find any problems, and gather ideas that will help create a better system.
b. Suggesting a Framework: Using what we learned from the studies, we'll suggest a detailed plan to make IoT in healthcare more secure. This plan will fix the problems we found and be strong, flexible, and useful in real healthcare situations.
c. Checking the Framework: We will check if our suggested plan works well by comparing it to well-known online standards like NIST and ISO. This means looking closely at each part of the plan and comparing it to what these standards say. The goal is to make sure our plan follows the best international practices and is strong enough to handle the security problems with IoT devices in healthcare.

3.4 DATA COLLECTION AND ANALYSIS

3.4.1 Data Collection

Because this research is using a qualitative way, we'll collect data by looking at existing studies, systems, and standards related to security for IoT in healthcare. This includes academic articles, reports, and existing systems and standards like NIST, ISO, and MITRE

ATT&CK, as shown in Figure 2 (Inclusion and Exclusion Criteria). The goal is to gather a lot of data to really understand how secure IoT is in healthcare right now, learn about the problems it faces, and see what solutions are suggested in existing studies and systems.

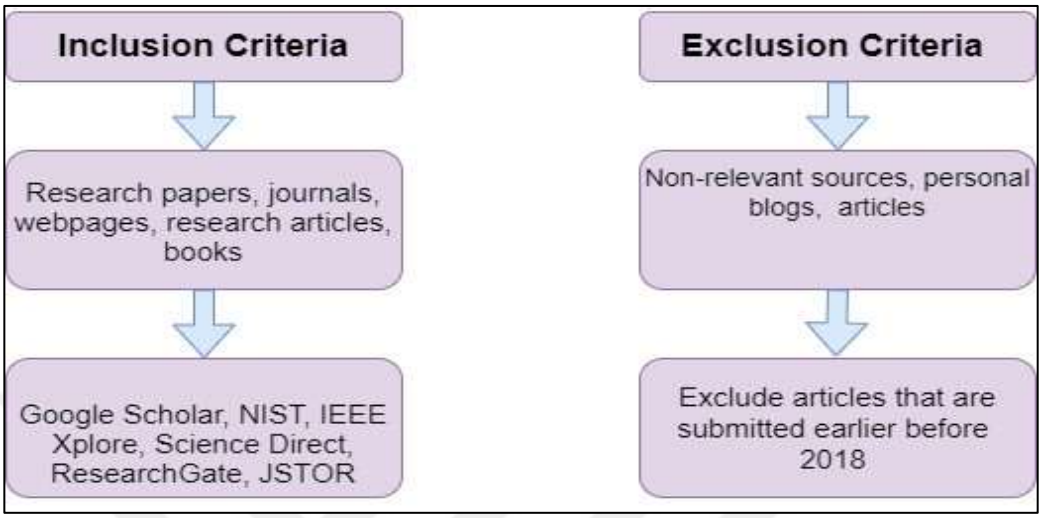

Figure 3.2: Outlines the Criteria for What Is Included And Excluded.

3.4.2 Prisma Methodology Diagram

The PRISMA diagram shows how we did this research. It gives a picture of the steps we took, from finding important studies and reports to including the ones that mattered the most.

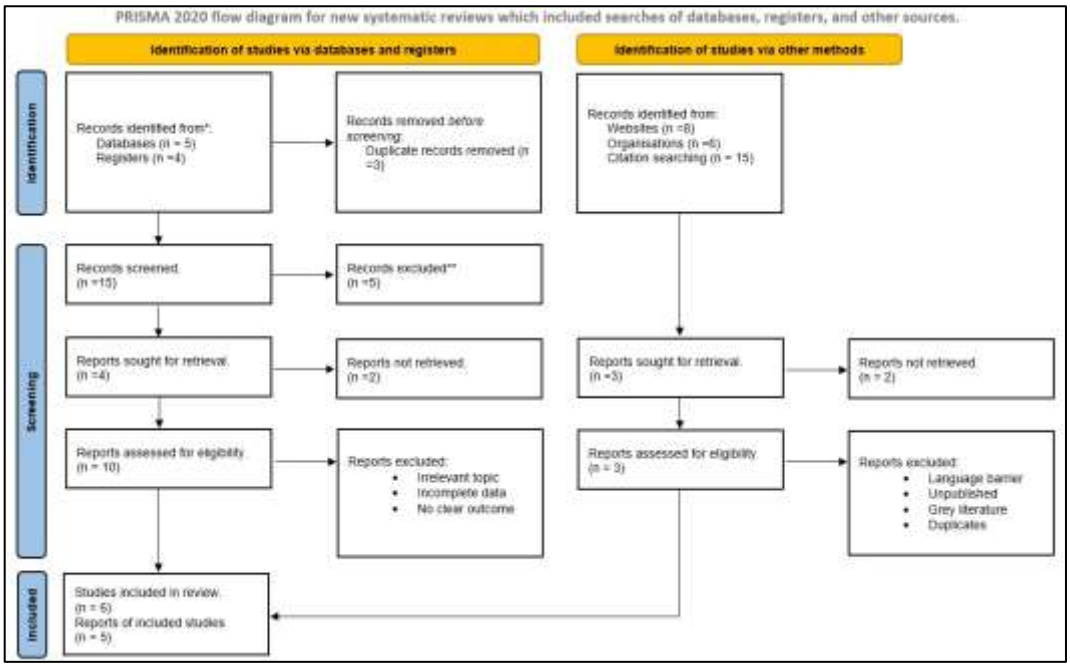

Figure 3.3: Displays the Prisma Methodology.

3.4.3 Data Analysis

We will do a few things to study the collected data:

a. Looking at the Content: We will carefully check and analyse the data to find important themes, challenges, and solutions related to IoT security in healthcare. This helps us understand how secure IoT is in healthcare now and find any problems or limits in the current ways.
b. Finding the Gaps: Based on the content analysis, we will look for specific areas where the current ways and systems are not enough. This involves comparing what we found in the content analysis with the requirements of well-known standards like NIST, ISO, and MITRE ATT&CK.
c. Creating a Framework: Using what we found in the content and gap analysis, we will create a detailed plan to make IoT in healthcare more secure. This plan will fix the problems we found and be strong, flexible, and useful in real healthcare situations.
d. Checking the Framework: We will check if our suggested plan works well by comparing it to well-known online standards like NIST, ISO, and MITRE ATT&CK. This means looking closely at each part of the plan and comparing it to what these standards say. The goal is to make sure our plan follows the best international practices and is strong enough to handle the security problems with IoT devices in healthcare.

4. PROPOSED FRAMEWORK

4.1 HEALTHCARE IOT SECURITY CHALLENGES

The healthcare field is excited about using devices connected to the Internet of Things (IoT), like medical wearables and linked medical tools. They want to improve patient care and make operations more effective. Healthcare can do things like monitoring patients from a distance, diagnosing issues early, and preventing diseases, especially for chronic ones like diabetes, lung disease, cancer, arthritis, and heart disease. However, as these devices get more connected, they face new security problems. This is because healthcare devices, like medical tools, wearables, and monitors, are at risk of cyber threats and dangers. Even though these connected devices bring many advantages, they also bring big threats to privacy and security [19]. The problems include keeping patient data private and secure, making sure devices can talk to each other safely, stopping unauthorized access, making sure devices work as they should, and keeping security measures updated in a quickly changing technology world. Also, many old ways of keeping IoT safe are not good enough against new threats and weaknesses. There's a need for models or frameworks to handle these big security issues with IoT devices, and there are still some gaps when it comes to security problems. It's important to work hard to solve these issues and make sure healthcare information and services are private, reliable, and always available.

4.2 SECURITY PROBLEMS IN HEALTHCARE IOT

a. Unauthorized Access: If people get into patients' health data without permission, mess with medical devices, or change data, it can really harm patients' health and safety.
b. Vulnerability to Attacks: IoT devices can be used to create botnets or be part of attacks, like man-in-the-middle attacks, making them a good target for cybercriminals.
c. Lack of a Good Security Plan: There's no proper plan or framework to handle big security issues with IoT devices, and there are still some gaps in dealing with security problems.

4.3 TRADITIONAL SIEM FEATURES

SIEM is a set of tools, like SolarWinds, ArcSight (now owned by Micro Focus), Splunk, IBM QRadar, and services that give a complete view of an organization's information security. Sometimes, it's made specifically for an organization's setup. SIEM systems quickly check security notifications from software and devices in an organization. These systems collect, save, study, and make reports on log information. They are important for dealing with security issues, doing detailed investigations, and following rules about security [12]. As shown in Table 1, SIEM solutions have many features that make them different from each other. Still, the basic features are the same for all of them, and these features include along with their reasons such as: [Details from Table 4.1 are not provided in the paragraph.]

Table 4.1: Lists Features Commonly Found In Traditional SIEM Systems.

Features	Reasons
Real-time Monitoring	SIEM tools keep a constant watch on what's happening in a company's network to find anything strange or suspicious.
Threat Detection	These solutions use different algorithms and established rules to find both known and unknown threats in the network.
Incident Response	These tools assist in automatically responding to a security problem. This might involve things like blocking certain IP addresses, turning off user accounts, and adjusting access controls.
Log Management	SIEM solutions gather and save log data from different places in the organization. Afterward, this data is used for analysis and creating reports.

4.4 PROBLEMS WITH CURRENT SIEM SYSTEMS

a. Hard to Use: SIEM systems are often hard to set up and need special skills to manage.
b. Expensive: Setting up and keeping a SIEM system can cost a lot, making it tough for smaller organizations to use.
c. Wrong Alerts: SIEM systems often show many wrong alerts, which can confuse security teams and make it hard to find real threats.
d. Slows Down: Gathering and studying a lot of log data can slow down the network and other computer resources.
e. Even with these problems, SIEM is an important tool for making an organization's cybersecurity better. It helps with real-time watching, finding threats, and dealing with cyber problems.

4.5 POTENTIAL SIEM INTEGRATION

a. Security Information and Event Management (SIEM) can bring a lot of benefits when integrated into healthcare IoT systems. SIEM tools analyse security alerts from applications and devices in real-time, which is very important in healthcare where patient data is sensitive, and monitoring patients' health happens right away.
b. Watching in Real-time and Spotting Threats: Thanks to the fast growth of technology, big data, and artificial intelligence, smart healthcare systems are here. These systems give detailed communication and home exposure reports and allow rehabilitation specialists and other experts to get involved. Integrating SIEM into healthcare IoT systems helps with real-time monitoring and finding threats quickly, which is vital for taking care of patients' health and keeping their data safe.
c. Keeping Health Records Safe: Combining blockchain and IoT is suggested for a safe way to store and check patient information. They've made a system called blockchain-based IoT-EHR that can automatically sense patient records and keep them safe [4]. SIEM integration can work together with this system by quickly checking security alerts and acting if needed.
d. Helping in Safe Healthcare with IoT: Telepresence robots are becoming more common in healthcare because they bring many benefits. But they have challenges in making important decisions while moving, needing a lot of training and smart planning [6].

Integrating SIEM can help by automatically dealing with security problems and making sure the right steps are taken when telepresence robots move.

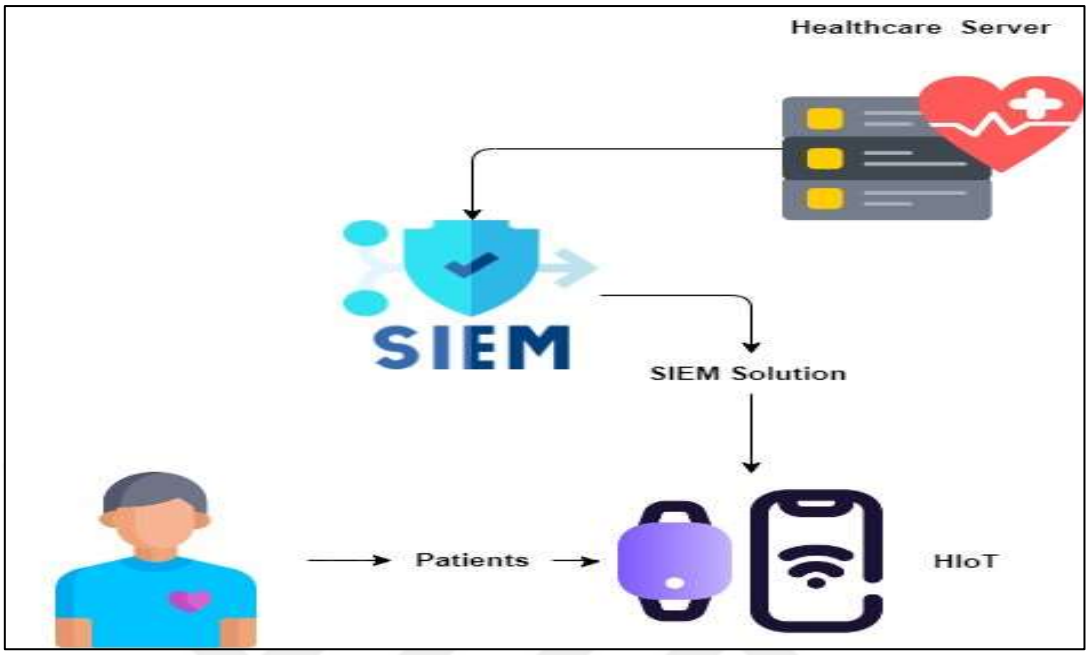

Figure 4.1: Shows the combination of SIEM and HIoT.

So, adding SIEM to healthcare IoT systems can help watch things right away, find threats, keep health records safe, and avoid problems in sustainable healthcare systems with IoT. But we need to think about the problems that can come with adding SIEM, like it being hard to use, expensive, showing wrong alerts, and slowing things down.

4.6 COMPREHENSIVE SECURITY FRAMEWORK FOR IOT DEVICES

This research suggests a way to combine Healthcare IoT and SIEM, and it has three main parts: The Healthcare Server, IoT Devices, and SIEM. The Healthcare Server keeps all the real-time health data from different devices and helps with quick medical actions. The IoT Devices are important because they smoothly connect to the server and give important health information. The SIEM part adds strong security features like finding threats, responding to problems, and collecting logs. This makes sure that the data moving between IoT devices, and the Healthcare Server is safe. This way of putting things together not only makes healthcare better but also makes the system stronger against possible security problems.

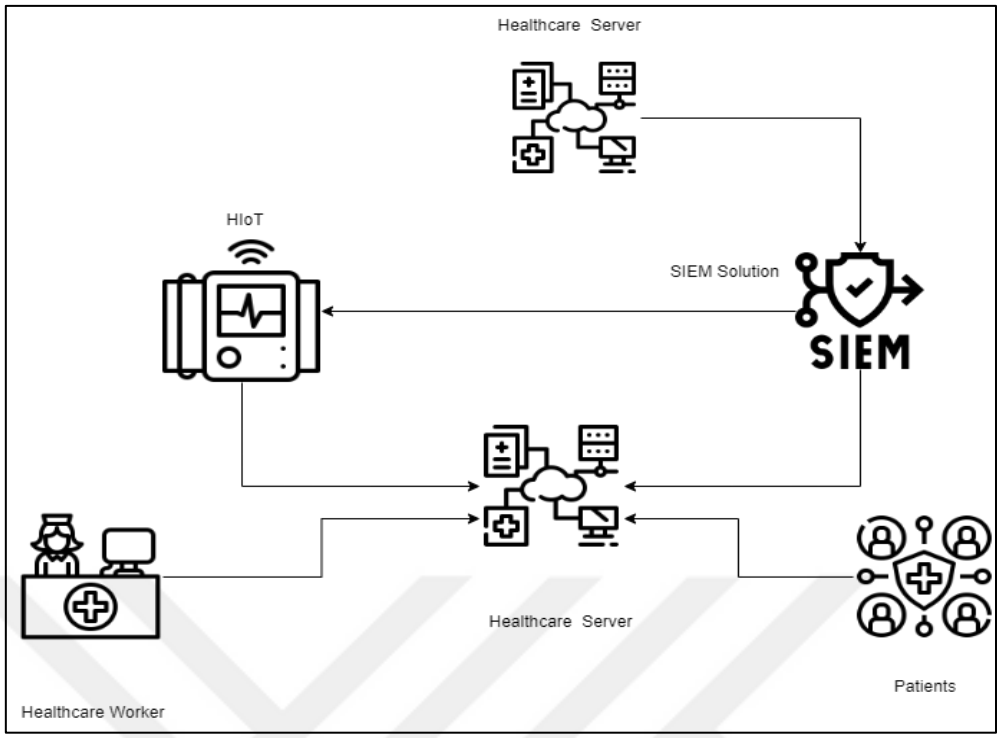

Figure 4.2: Illustrates the Suggested Framework, where HIOT and SIEM are Integrated.

As people use Patient Monitoring Devices, these IoT gadgets will keep collecting important health information in real-time. This data, covering lots of health details, will then be sent safely to the Healthcare Server. They'll use advanced ways to lock up the data while it's moving to make sure it's safe from any potential problems, keeping patients' private health info safe. When the data reaches the Healthcare Server, which is like a big storage place, it gets another layer of protection by using encryption, making sure it stays safe when it's not moving. This server doesn't just keep the data but also helps authorized healthcare workers and patients get to it. To make sure only the right people can see the data, they use something called MFA, which needs users to prove who they are in multiple ways before they can see the information. While the Healthcare Server and IoT devices are busy with collecting and storing data, the SIEM part is like the security backbone of this system. It keeps watching the data going between IoT devices and the server, finding and flagging any strange or potentially harmful things. With the Log Collection feature, every time something happens with the data, like someone trying to get to it or system events, it gets written down in detail, making a complete record. The Event Correlation feature goes through these records, connecting events to figure out patterns or strange things, which the Threat Detection part checks. If a threat is found, the Incident Response part takes over, following a plan to stop

the threat and keep the system safe. Also, the SIEM makes sure to regularly check and test the Healthcare Server's security with Security Audits and Penetration Testing, fixing any problems before they become big issues. Also, the Network Segmentation feature splits the network into parts, keeping different sections separate to make it harder for problems to spread. If there's a security problem, a clear plan in the SIEM, called an Incident Response Plan, will guide what needs to be done right away, making sure the response is quick and effective. When this system is up and running, it not only makes managing healthcare data easier but also sets a high standard for keeping that data safe, making sure patients' health information is both available and protected.

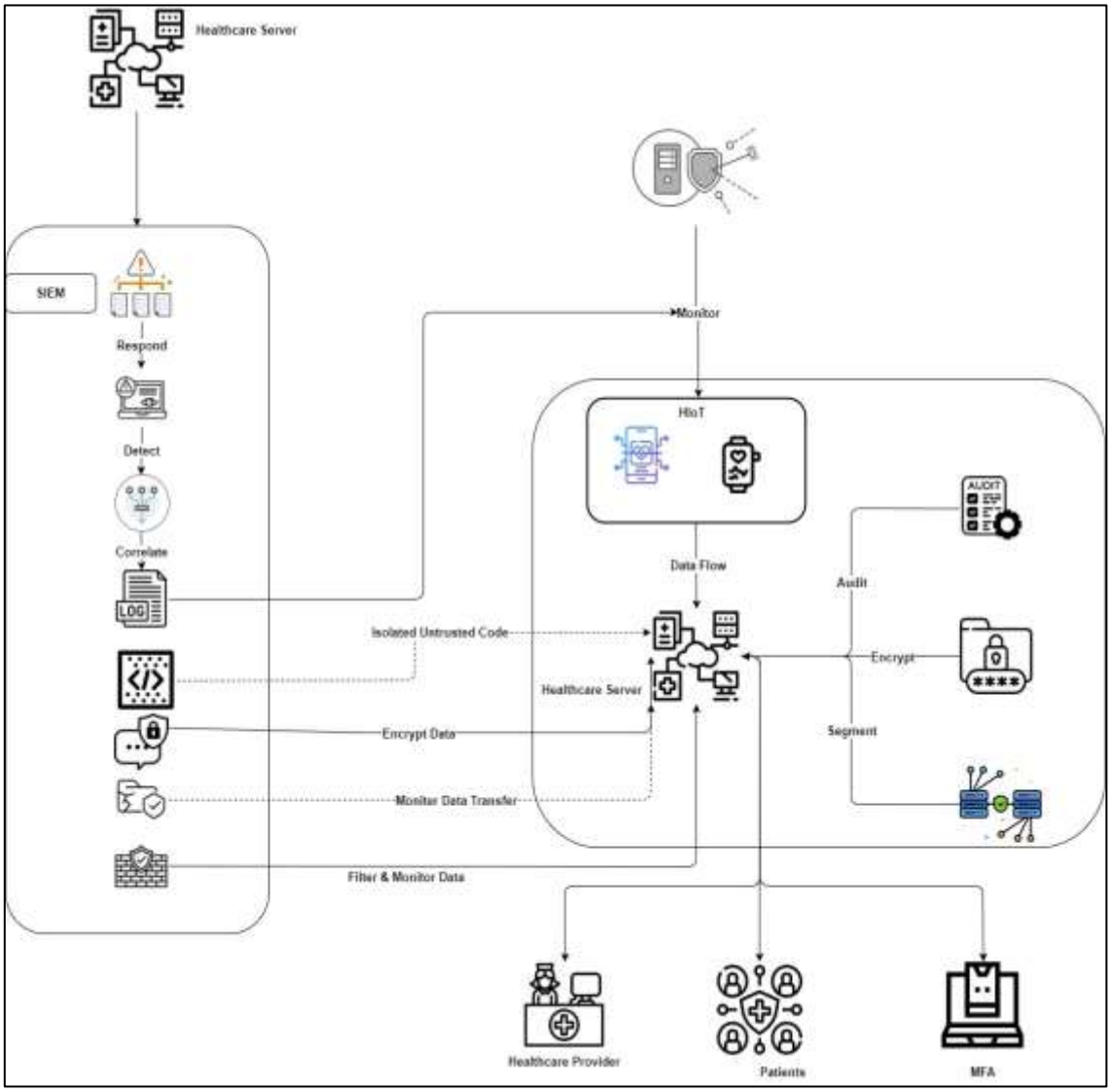

Figure 4.3: Depicts The Architecture Of The Framework.

Table 4.2 Shows What Makes Up the Framework.

Component	Description
Healthcare Server	A central storage holding health data gathered by monitoring devices, allowing healthcare workers and patients to access the information.
Patient Monitoring Devices	Devices that keep track of patients' health in real-time and send the gathered data to the Healthcare Server.
Healthcare Workers	Healthcare professionals who check and understand the data from the Healthcare Server to provide patient care.
Patients	People whose health information is being watched and stored. They can check their own data from the Healthcare Server.
Multi-Factor Authentication (MFA)	A security measure that needs different forms of verification to get into the Healthcare Server, making sure only authorized users can access sensitive health data.
Endpoint Detection and Response (EDR)	Keeps an eye on endpoints like Patient Monitoring Devices to find and deal with threats, stopping possible breaches.
Network Segmentation	Divides the network to separate different sections, making it harder for threats to spread and reducing the chance of attacks.
Data Encryption	Protects the data stored in the Healthcare Server by turning it into a secret code, keeping it confidential and stopping unauthorized access even if someone tries to intercept it.
Security Audits	Consistently examines and tests the Healthcare Server to discover and address security weaknesses.
Incident Response Plan	Describes what to do if there's a security problem. This is carried out by the Incident Response part of the SIEM.
SIEM	A system that instantly analyses security alerts created by both hardware and software.
Log Collection	Gathers logs from Patient Monitoring Devices and forwards them to the Event Correlation part for analysis.
Event Correlation	Studies and links gathered events to find patterns or unusual things, helping to detect threats.
Threat Detection	Looks at linked events to find threats, making sure there's a quick response to potential security issues.

Table 4.2 Shows What Makes Up the Framework "Table Continued".

Incident Response	Takes action when incidents are found by following the Incident Response Plan and updating security rules.
Secure Communication	Makes sure that data moving between IoT devices, and the server is protected by encrypting it using protocols like TLS. This ensures safety from eavesdropping or tampering.
Sandboxing	Runs programs or code that can't be trusted in a separate space, stopping them from causing any harm to the main system.
Data Loss Prevention (DLP)	Watches and manages the data moving through the organization's network, stopping any unauthorized leaks or breaches.
Firewall & Intrusion Prevention System (IPS)	Blocks harmful internet traffic and stops attacks immediately, serving as the initial defence against possible cyber threats.

4.7 WORKING OF THE FRAMEWORK

a. This plan is made to create a safe and effective healthcare space, especially thinking about how to add IoT devices to healthcare.
b. Getting and Keeping Data Safe: Devices watching patients all the time gather health info and send it to a place called the Healthcare Server. Then, Healthcare Workers and Patients can see this data.
c. Staying Safe: To keep data safe and in good shape, a few safety steps are taken:
    i. MFA makes sure only the right people can get in.
    ii. EDR looks for problems with the devices.
    iii. Network Segmentation keeps parts of the network separate.
    iv. Data Encryption makes sure data is private.
    v. Regular Security Audits find and fix problems.
d. Adding SIEM: The SIEM system is important in keeping the whole plan safe. It collects logs, connects events, finds threats, and follows a plan to fix things if needed. Other safety parts like Secure Communication, Sandboxing, DLP, and Firewall & IPS make things even safer.
e. Fixing Problems: If something bad happens, the SIEM's Incident Response part takes over, following a plan to stop the problem and make things normal again.

f. Keeping an Eye and Making Things Better: The plan is made to always be changing. Regular safety checks, testing, and adding what's learned from threats make sure the plan is up to date with the latest safety rules and ways of doing things.

Basically, this plan looks at IoT safety in healthcare in a big way, making sure patient info is collected, kept, and looked at in a safe and effective way.

5. ANALYSIS AND STANDARDIZATION

Keeping patient info safe is super important in healthcare. As more patient info goes digital and we use fancy medical devices, we really need a strong plan to keep everything safe from cyber problems. This part of the plan checks if our idea fits in with the rules that are already there, making sure it works well against the problems we might face now.

5.1 STANDARDS JUSTIFICATION

The next big thing we need to do with our plan is to see how it fits with rules that are already there, like NIST and The MITRE ATT&CK framework. This framework is like a big library of things bad guys might do, based on what's really happening in the world.

Table 5.1: Shows How Things Match Up with MITRE ATT&CK, NIST SP 800-53 Rev. 5, And ISO/IEC 27001 Standards.

Framework Component	**MITRE ATT&CK Mapping**	**NIST SP 800-53 Rev. 5 Mapping**	**ISO/IEC 27001 Mapping**	**Description**
Healthcare Server	Storing and handling data.	Controlling access.	Managing assets. (A.8)	Keeping patient data in one place with controlled access.
Patient Monitoring Devices	Gathering information	Keeping systems and communication safe.	Taking care of belongings. (A.8)	Gadgets gathering patient information in the moment.
Multi-Factor Authentication (MFA)	Getting permission to use something.	Recognizing and verifying who you are.	Deciding who can use something. (A.9)	Makes sure only the right people can get to important information.
Endpoint Detection and Response (EDR)	Protecting the devices, you use.	Keeping the system and information safe and whole.	Handling situations where information security is at risk. (A.16)	Watches out for and deals with dangers on individual devices.
Network Segmentation	Protecting the network, you use.	Guarding systems and communication**.**	Keeping communications safe. (A.13)	Dividing the network to make it harder for attacks to happen.
Data Encryption	Keeping information safe.	Guarding the system and communication.	Using codes to keep things secure. (A.10)	Turns information into secret code to keep it private.
Security Audits and Penetration Testing	Checking how safe something is called a security assessment.	Evaluating, allowing, and keeping an eye on things (CA).	Following the rules (A.18).	Finds and repairs security problems.

Table 5.1: Shows how Things Match up with MITRE ATT&CK, NIST SP 800-53 Rev. 5, and ISO/IEC 27001 Standards "Table Continued".

Incident Response Plan	Reacting to and dealing with problems (Incident Response).	Reacting to and handling incidents (IR).	Dealing with problems related to information security (Information Security Incident).	Describes the necessary actions for a quick and efficient process.
			Handling things (A.16).	Reacting to security problems.
SIEM	Watching out for security issues.	Checking and keeping track of things (AU).	Watching and checking things (A.12).	Detects threats in real time and can respond to incidents quickly.
Secure Communication	Protecting the network.	Keeping systems and communications safe (SC).	Making sure communications are secure (A.13).	Makes sure information travels securely between devices and servers.
Sandboxing	Protecting against harmful computer programs.	Ensuring that systems and information are reliable (SI).	Getting, building, and taking care of systems (A.14).	Keeps unsafe code separate to stop possible dangers.
Data Loss Prevention (DLP)	Keeping information safe.	Guarding media (MP).	Keeping things secure during operations (A.12).	Watches and manages how data moves through the network.
Firewall & IPS	Guarding the network.	Keeping systems and communications safe (SC).	Communication Security (A.13) is about keeping information safe and private when it's shared.	Filters and monitors traffic to stop unauthorized access.

Table 5.1 outlines a solid strategy to safeguard healthcare data. It incorporates key elements from MITRE ATT&CK, NIST SP 800-53 Rev. 5, and ISO/IEC 27001 standards. The primary goal is to secure patient information on healthcare servers, ensuring that only authorized individuals can access it. Continuous monitoring devices collect real-time data from patients. To enhance data security and restrict access to authorized personnel, measures like multi-factor authentication (MFA) and endpoint detection and response (EDR) are employed. The network is divided, and encryption is used to keep data confidential. Regular checks and tests identify potential issues, with a quick response plan in place for security problems. Incorporating Security Information and Event Management (SIEM) ensures constant vigilance for problems, and secure methods are used for data transmission. Additional safeguards include sandboxing to prevent malicious activities, tools for monitoring data transfers, and robust protections against unauthorized access attempts. These practices align with established rules and standards such as NIST, MITRE ATT&CK, and others.

5.2 MINIMUM REQUIREMENTS FOR FRAMEWORK

Making a cybersecurity plan, especially for healthcare, needs to follow important rules for the best security, trust, and efficiency. The plan should put patient info in one safe place with strict control, making sure only the right people can see sensitive info. Mixing edge computing with blockchain tech is important to meet needs like lasting a long time, being strong against network problems, and building trust even when the network changes a lot. Also, with tech changing fast and more cybercrimes, we need to keep updating and training systems that look out for bad stuff to stay effective. Following global rules, like the ones in the EU NIS Directive, is crucial to make sure the plan meets global cybersecurity needs. Basically, any plan should cover everything, be able to change, and keep up with the newest tech and rules to keep healthcare data safe.

5.3 INTERPRETATION ON FINDINGS

RQ1: Connecting Security Information and Event Management (SIEM) systems with healthcare IoT devices can bring many advantages. One big plus is better monitoring. Systems like FETCH, as explained by [44], work with edge computing devices and can help monitor real-life healthcare situations, like keeping an eye on heart disease.

These systems use deep learning and automated monitoring to work better. Another good thing is handling the tons of data coming from IoT healthcare systems more efficiently. Smart devices and the Cloud can struggle with this data, as pointed out But Fog computing, a new layer, can process this data closer to where it's made, making things faster and better. IoT data analytics in healthcare has a lot of potential. Share a framework for smart video surveillance of patients. This kind of framework, when mixed with IoT systems, can really help find critical patients, especially in emergencies. But, bringing together SIEM and healthcare IoT has some challenges. Safety is a big worry. Because IoT devices use wireless communication and are spread out, they can be open to bad attacks. Also, with more health data made, keeping patient info private is super important. If unauthorized people get this info, it can cause big ethical and legal problems. To solve these issues, we can use the strengths of SIEM systems. They can do real-time checks on security alerts from healthcare IoT devices [44]. They can see different events and figure out if there's a pattern showing a security problem. If there's anything strange in security, SIEM systems can start automated responses to stop possible threats.

RQ2: Building a complete security plan for healthcare IoT devices means dealing with known issues and combining the best practices and key safety steps. From what we've learned in the chapters provided:

a. Handling Known Security Issues:

Healthcare has special problems, especially with many IoT devices around. These devices are different, and because healthcare info is sensitive, they become main targets for cyber-attacks. Fixing these problems needs a many-sided plan like:

a. Checking if devices are real

b. Making sure data is secret

b. Using the Best Practices:

Keeping the software updated is super important. It makes sure that any problems in the system are fixed quickly. Also, teaching healthcare workers about safety is important. If they know the best safety practices, it can lower the chances of accidents caused by people.

c. Putting in Key Safety Steps:

A good safety plan mixes in different safety steps:

- Access Controls: Make rules about who can get to the data. This makes sure healthcare workers only get to the data they need. These stops data problems and makes sure only allowed people can see patient info.

- Anomaly Detection Systems: These are important for the safety plan. They keep an eye on IoT devices all the time. If they see anything strange or bad, they tell the right people straight away.

So, a good safety plan for healthcare IoT devices must cover everything—both tech stuff and things people do. By dealing with known issues, using the best practices, and putting in key safety steps, we can keep healthcare IoT devices safe from many types of safety problems.

RQ3: The new safety plan has a big effect on how safe healthcare IoT devices are, especially in finding threats accurately and responding to incidents quickly:

a. Finding Threats Accurately:

The plan has systems that always watch what IoT devices are doing. This watchful eye makes sure any weird or suspicious stuff gets noticed quickly. Using smart computer programs and learning machines, the plan makes finding threats much better. The chapters also talk about using special ways to check if people trying to use devices are really who they say they are. This makes sure only the right people can use the devices.

b. Responding to Incidents Quickly:

The plan uses lots of steps to make sure possible threats are found and fixed fast. Instant alerts made by the watching systems help healthcare workers and IT teams act right away, stopping possible risks. The chapters also say that keeping the software up to date is super important. This makes sure problems are fixed quickly, so there's less time for something bad to happen.

In real healthcare places, this plan makes a big difference. It not only makes sure patient info is safe but also keeps IoT devices working well. This is super important for giving

the best care to patients. By dealing with tech stuff and challenges with people, the plan is a full solution to the safety worries about healthcare IoT devices.

6. CONCLUSION AND FUTURE WORK

The rise of Internet of Things (IoT) devices in healthcare has significantly changed how patients are cared for and diagnosed. However, with their increasing presence, security concerns have also risen. This study delves into these issues and proposes a detailed security plan as a solution. This part critically looks at the study's discoveries and the suggested system, putting them in the larger academic discussion. The security plan highlighted here focuses on multiple layers of protection. This aligns with the findings of Ahmadi-Assalemi et al. (2019), who talked about the complex challenges brought by the combination of IoT and Hyperphysical Systems (CPS) in various sectors. Their suggestion for a Security-by-Design framework matches the proactive steps promoted in this study. Additionally, their incorporation of forensic readiness and liability attribution supports the holistic nature of the presented plan.

The study's attention to strong authentication, data encryption, access controls, and anomaly detection is timely and essential. Morales also stressed the limitations of traditional security tools like Intrusion Detection Systems (IDS) and Security Information and Event Management Systems (SIEM) in handling advanced IoT threats. Their exploration of identity attacks, especially the Clone ID attack, emphasizes the need for advanced, Artificial Intelligence-driven protective frameworks, a sentiment echoed in this study. Implementing the proposed plan in real healthcare settings has significant practical implications. Insights from Button and Sari's work on the difficulties of integrating security measures in older systems, particularly in smart grids, are relevant. Their distinction between operational failures and cybersecurity incidents offers a valuable perspective, especially in the critical context of healthcare.

In summary, this research provides a comprehensive approach to the security challenges brought by healthcare IoT devices. The plan's focus on proactive measures, advanced threat detection, and practical usability makes it a significant contribution to both academic and practical aspects. However, the ever-changing nature of technological threats requires continuous research and adaptation. Future studies could explore the deeper integration of machine learning in threat detection, the impact of user behaviour on security, and the difficulties of setting global standards in healthcare IoT security.

6.1 FUTURE WORK

The research journey had its share of challenges, and this section openly discusses the limitations encountered during the study, providing an honest account for readers and future researchers.

a. Scope of IoT Devices: The study focused on a subset of healthcare IoT devices, and the findings may not apply universally to all such devices. The proposed security framework, while comprehensive, needs evaluation across the entire range of devices.
b. Real-world Implementation: The security framework, though robust in design, exists in a theoretical form. Real-world healthcare settings, with their unique challenges, might present unforeseen obstacles during implementation, a consideration for future work.
c. Rapid Technological Advancements: Technology, especially in IoT, is dynamic, with new devices, threats, and solutions emerging regularly. While the research offers a current snapshot, updates may be necessary to remain relevant amid rapid technological changes.
d. Data Collection: The study relied on existing datasets and literature, introducing potential biases. The absence of primary data collection, like interviews or surveys, may have limited insights into practical challenges faced by healthcare professionals.
e. Geographical Limitations: The research mainly focused on specific regions, and differences in culture, regulations, and technology across countries could impact the proposed framework's global applicability.
f. Interdisciplinary Challenges: Navigating the intersection of healthcare and technology introduced challenges. While efforts were made to bridge the knowledge gap, there may be nuances specific to each field not fully captured, as mentioned by [9].

Despite these limitations, the study offers valuable insights and solutions to healthcare IoT device security challenges. It's crucial to consider these limitations when interpreting the findings, and future research can build on this foundation, addressing the outlined constraints and refining proposed solutions.

6.2 CONCLUSIONS

The transformation of healthcare through digital means, especially with the use of IoT devices, has opened new possibilities. These devices offer benefits like remote patient

monitoring and advanced diagnostics, reshaping how medical care is delivered. However, along with these advancements, there are complex challenges, especially regarding the security of these devices. This study aimed to understand, tackle, and propose solutions to these challenges.

Our exploration began by looking into the potential benefits and limitations of combining Security Information and Event Management (SIEM) systems with healthcare IoT devices. While SIEM systems offer improved detection and response capabilities, integrating them with the diverse world of IoT devices comes with its challenges.

Building on this, the research moved on to design a comprehensive security framework tailored for healthcare IoT devices. This framework, shaped by identified challenges and best practices, included key security measures like authentication mechanisms and anomaly detection. The goal was to strengthen the security of these devices, ensuring the integrity of patient data and the proper functioning of the devices.

Assessing the impact of this proposed framework, the study explored its real-world implications. The findings showed promise, indicating improved threat detection accuracy and a quicker incident response time. These results highlight the potential of the framework not only to address current security concerns but also to adapt to future challenges.

However, like any research, this study had its limitations. From the scope of IoT devices considered to the challenges of real-world implementation, these limitations provide opportunities for future research and refinement.

In conclusion, the journey of this research has been both enlightening and challenging. The world of healthcare IoT is vast, dynamic, and full of potential. While this study offers a roadmap to navigate its security challenges, the journey is ongoing. As technology evolves and new possibilities emerge, continuous research, adaptation, and collaboration will guide us to realize the promise of healthcare IoT in its most secure form.

REFERENCES

[1] H. Ahonen, "Tämä kaikki Vastaamo-tapauksesta nyt tiedetään: Avoimia kysymyksiä on paljon – yhtenä suurimmista rikoksen tekijä," *Aamulehti*, 26-Oct-2020. [Online]. Available: https://www.aamulehti.fi/rikos/art-2000007419612.html. [Accessed: 27-Apr-2024].

[2] V. Adat and B. B. Gupta, "Security in Internet of Tings: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, no. 3, pp. 423–441, 2018.

[3] G. Ahmadi-Assalemi *et al.*, "Digital Twins for Precision Healthcare," in *Advanced Sciences and Technologies for Security Applications*, Cham: Springer International Publishing, 2020, pp. 133–158.

[4] S. Alam *et al.*, *An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring*. .

[5] A. A. T. Al-Khazaali and S. Kurnaz, "Study of integration of blockchain and Internet of Things (IoT): an opportunity, challenges, and applications as medical sector and healthcare," *Applied Nanoscience*, vol. 13, pp. 1531–1537, 2023.

[6] A. A. Altalbe, M. N. Khan, and M. Tahir, *Design of a Telepresence Robot to Avoid Obstacles in IoT-Enabled Sustainable Healthcare Systems*. .

[7] M. Arefin, M. M. Rahman, M. Hasan, and R. Ahmed, *A Topical Review on Enabling Technologies for the Internet of Medical Things: Sensors, Devices, Platforms, and Applications. Preprints. Preprints*. .

[8] Z. Baghizadeh, D. Cecez-Kecmanovic, and D. Schlagwein, "Review and critique of the information systems development project failure literature: An argument for exploring information systems development project distress," *J. Inf. Technol.*, p. 026839621983201, 2019.

[9] T. Ban, T. Takahashi, S. Ndichu, and D. Inoue, *Breaking Alert Fatigue: 10. AI-Assisted SIEM Framework for Effective Incident Response*. .

[10] M. Bano and D. Zowghi, “Users’ involvement in requirements engineering and system success,” in *2013 3rd International Workshop on Empirical Requirements Engineering (EmpiRE)*, 2013.

[11] M. Bano and D. Zowghi, “A systematic review on the relationship between user involvement and system success,” *Inf. Softw. Technol.*, vol. 58, pp. 148–169, 2015.

[12] V. S. Barletta, D. Caivano, M. D. Vincentiis, A. Ragone, M. Scalera, and M. Martín, *V-SOC4AS: A Vehicle-SOC for Improving Automotive 12*. .

[13] M. Baslyman, D. Amyot, and Y. Alshalahi, “Lean healthcare processes: Effective technology integration and comprehensive decision support using requirements engineering methods,” in *2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH)*, 2019.

[14] H. Benbya, N. Nan, H. Tanriverdi, and Y. Yoo, “Complexity and information systems research in the emerging digital world,” *MIS Quarterly: Management Information Systems*, 2020.

[15] L. L. Boca, E. M. Ciortea, C. Boghean, A. Begov-Ungur, F. Boghean, and V. T. Dădârlat, “An IoT system proposed for higher education: Approaches and challenges in economics, computational linguistics, and engineering,” *Sensors (Basel)*, vol. 23, no. 14, 2023.

[16] S. K. Boell and D. Cecez-Kecmanovic, *what is an information system? Proceedings of the Annual Hawaii International Conference on System Sciences*. 2015.

[17] S. Boopathi, *Dynamics of Swarm Intelligence Health Analysis for the Next Generation Publisher: IGI Global Samapth Boopathi*. IGI Global Samapth Boopathi.

[18] N. Carter, D. Bryant-Lukosius, A. DiCenso, J. Blythe, and A. J. Neville, “The use of triangulation in qualitative research,” *Oncol. Nurs. Forum*, vol. 41, no. 5, pp. 545–547, 2014.

[19] C. Anil and T. Hayajneh, “Chacko Anil and Thaier Hayajneh etal., licensed to EAI.”

[20] R. M. Czekster, P. Grace, C. Marcon, F. Hessel, and S. C. Cazella, “Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT,” *Appl. Sci*, vol. 2023.

[21] J. L. Dargan, J. S. Wasek, and E. Campos-Nanez, “Systems performance prediction using requirements quality attributes classification,” *Requir. Eng.*, vol. 21, no. 4, pp. 553–572, 2016.

[22] K. R. Darshan and K. R. Anandakumar, “A comprehensive review on usageof Internet of Things (IoT) in healthcare system,” in *International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, 2015, pp. 132–136.

[23] C. Eken and H. Eken, “Security threats and recommendation in IoT healthcare,” in *Proceedings of the 9th EUROSIM Congress on Modelling and Simulation, EUROSIM 2016, The 57th SIMS Conference on Simulation and Modelling SIMS 2016*, 2018.

[24] “Julkiset hankinnat,” *Elinkeinoelämän keskusliitto*, 13-Jul-2020. [Online]. Available: https://ek.fi/tavoitteemme/yrityslainsaadanto/julkiset-hankinnat/. [Accessed: 27-Apr-2024].

[25] U. H. Graneheim, B.-M. Lindgren, and B. Lundman, “Methodological challenges in qualitative content analysis: A discussion paper,” *Nurse Educ. Today*, vol. 56, pp. 29–34, 2017.

[26] J. Gustafsson, *Single case studies vs. multiple case studies: A comparative study*. Sweden, 2017.

[27] Y.-C. Hsiao, M.-H. Wu, and S. Li, “Elevated performance of the smartcity-A case study of the IoT by innovation mode,” *IEEE Transactions on Engineering Management*, vol. 68, no. 5, pp. 1461–1475.

[28] H. Hyppönen, O. Pentala-Nikulainen, and A. Aalto, “Sosiaali- ja terveydenhuollon sähköinen asiointi 2017: Kansalaisten kokemukset ja tarpeet,” *Terveyden ja hyvinvoinnin laitos*, vol. 3, 2018.

[29] S. Jabbar, F. Ullah, S. Khalid, M. Khan, and K. Han, “Semantic interoperabilityin heterogeneous IoT infrastructure for healthcare,” *Wireless Communications and Mobile Computing*, 2017.

[30] M. Kauppinen, M. Vartiainen, J. Kontio, S. Kujala, and R. Sulonen, *implementing requirements engineering processes throughout organizations: Success factors and challenges. Information and Software Technology*. 2004.

[31] S. Kujala, M. Kauppinen, L. Lehtola, and T. Kojo, “The role of user involvement in requirements quality and project success,” in *13th IEEE International Conference on Requirements Engineering (RE’05)*, 2005.

[32] J. Lagsten and A. Andersson, “Use of information systems in social work- challenges and an agenda for future research,” *European Journal of Social Work*, 2018.

[33] A. S. Lee, M. Thomas, and R. L. Baskerville, “Going back to basics in design science: from the information technology artifact to the information systems artifact: From the IT artifact to the IS artifact,” *Inf. Syst. J.*, vol. 25, no. 1, pp. 5–21, 2015.

[34] D. D. López *et al.*, *Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM Wireless Communications and Mobile Computing*. .

[35] R. A. Majid, N. L. M. Noor, W. A. W. Adnan, and S. Mansor, “A survey on user involvement in software Development Life Cycle from practitioner’s perspectives,” in *5th International Conference on Computer Sciences and Convergence Information Technology*, 2010.

[36] L. E. G. Martins and T. Gorschek, “Requirements engineering for safetycritical systems: A systematic literature review,” in *Information and Software Technology*, 2016.

[37] N. Pantelis *et al.*, “Developing an infrastructure for secure patient summary exchange in the EU context: Lessons learned from the KONFIDO project,” *Health Informatics Journal*.

[38] M. S. Rakha, L. Lapczyk, C. Dafnas, and P. Martin, “Addressing the security challenges of big data analytics in healthcare research,” *Int. J. Commun. Netw. Syst. Sci.*, vol. 15, no. 08, pp. 111–125, 2022.

[39] N. Sultana and M. Tamanna, “Exploring the benefits and challenges of Internet of Things (IoT) during Covid-19: A case study of Bangladesh,” *Discover Internet of Things”*, vol. 1, no. 1, pp. 20–2021.

[40] H. Chi, W. Zhou, and S. Piramuthu, “Internet of Things (IoT)in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review,” *Decision Support Systems*, vol. 108, pp. 79–95, 2018.

[41] V. Aivaliotis, K. Tsantikidou, and N. Sklavos, “IoT-based multi-sensor healthcare architectures and a lightweight-based privacy scheme,” *Sensors (Basel)*, vol. 22, no. 11, p. 4269, 2022.

[42] G. Xu, “IoT-Assisted ECG Monitoring Framework with Secure Data Transmission for Health Care Applications,” *IEEE Access: Practical Innovations”, Open Solutions*, vol. 8.

[43] K. Ylönen *et al.*, “Sosiaalialan asiakastietojärjestelmissä paljon parannettavaa: käyttäjäkokemukset 2019,” *Finn. J. eHealth welfare*, vol. 12, no. 1, pp. 30–43, 2020.

[44] A. Verma, S. Prakash, V. Srivastava, A. Kumar, and S. C. Mukhopadhyay, “Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review,” IEEE Sensors Journal, vol. 19, no. 20, pp. 9036–9046, Oct. 2019, doi: https://doi.org/10.1109/jsen.2019.2922409.