Division of Biomedical Engineering

Department of Human Biology

University of Cape Town

Project Title

Security for networked smart healthcare systems: A systematic review

Dissertation

MPhil in Health Innovation

Perfect Nyamwezi Ndarhwa (NDRNYA002)

Supervisor: Dr Bessie Malila

Posthumous supervisor: Prof Tania Douglas

Date: 02 July 2022

Declaration

I, Nyamwezi Parfaite Ndarhwa, hereby declare that the work on which this dissertation/thesis is based is my original work (except where acknowledgements indicate otherwise) and that neither the whole work nor any part of it has been, is being, or is to be submitted for another degree in this or any other university.

I empower the university to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever.

Signature: Signed by candidate

Date: 02 July 2022

Abstract

Background and Objectives

Smart healthcare systems use technologies such as wearable devices, Internet of Medical Things and mobile internet technologies to dynamically access health information, connect patients to health professionals and health institutions, and to actively manage and respond intelligently to the medical ecosystem's needs. However, smart healthcare systems are affected by many challenges in their implementation and maintenance. Key among these are ensuring the security and privacy of patient health information. To address this challenge, several mitigation measures have been proposed and some have been implemented. Techniques that have been used include data encryption and biometric access. In addition, blockchain is an emerging security technology that is expected to address the security issues due to its distributed and decentralized architecture which is similar to that of smart healthcare systems. This study reviewed articles that identified security requirements and risks, proposed potential solutions, and explained the effectiveness of these solutions in addressing security problems in smart healthcare systems.

Methods

This review adhered to the Preferred Reporting Items for Systematic Reviews and Meta-analysis (PRISMA) guidelines and was framed using the Problem, Intervention, Comparator, and Outcome (PICO) approach to investigate and analyse the concepts of interest. However, the comparator is not applicable because this review focuses on the security measures available and in this case no comparable solutions were considered since the concept of smart healthcare systems is an emerging one and there are therefore, no existing security solutions that have been used before. The search strategy involved the identification of studies from several databases including the Cumulative Index of Nursing and Allied Health Literature (CINAL), Scopus, PubMed, Web of Science, Medline, Excerpta Medical database (EMBASE), Ebscohost and the Cochrane Library for articles that focused on the security for smart healthcare systems. The selection process involved removing duplicate studies, and excluding studies after reading the titles, abstracts, and full texts. Studies whose records could not be retrieved using a predefined selection criterion for inclusion and exclusion were excluded. The remaining articles were then screened for eligibility. A data extraction form was used to capture details of the screened studies after reading the full text. Of the searched databases, only three yielded results when the search strategy was applied, i.e., Scopus, Web of science and Medline, giving a total of 1742 articles. 436 duplicate studies were removed. Of the remaining articles, 801 were excluded after reading the title, after which 342 after were excluded after reading the abstract, leaving 163, of which 4 studies could not be retrieved. 159 articles were therefore screened for eligibility after reading the full text. Of these, 14 studies were included for detailed review using the formulated research questions and the PICO framework. Each of the 14 included articles presented a description of a smart healthcare system and identified the security requirements, risks and solutions to mitigate the risks. Each article also summarized the effectiveness of the proposed security solution.

Results

The key security requirements reported were data confidentiality, integrity and availability of data within the system, with authorisation and authentication used to support these key security requirements. The identified security risks include loss of data confidentiality due to eavesdropping in wireless communication mediums, authentication vulnerabilities in user devices and storage servers, data fabrication and message modification attacks during transmission as well as while the data is at rest in databases and other storage devices. The proposed mitigation measures included the use of biometric accessing devices; data encryption for protecting the confidentiality and integrity of data; blockchain technology to address confidentiality, integrity, and availability of data; network slicing techniques to provide isolation of patient health data in 5G mobile systems; and multi-factor authentication when accessing IoT devices, servers, and other components of the smart healthcare systems. The effectiveness of the proposed solutions was demonstrated through their ability to provide a high level of data security in smart healthcare systems. For example, proposed encryption algorithms demonstrated better energy efficiency, and improved operational speed; reduced computational overhead, better scalability, efficiency in data processing, and better ease of deployment.

Conclusion

This systematic review has shown that the use of blockchain technology, biometrics (fingerprints), data encryption techniques, multifactor authentication and network slicing in the case of 5G smart healthcare systems has the potential to alleviate possible security risks in smart healthcare systems. The benefits of these solutions include a high level of security and privacy for Electronic Health Records (EHRs) systems; improved speed of data transaction without the need for a decentralized third party, enabled by the use of blockchain. However, the proposed solutions do not address data protection in cases where an intruder has already accessed the system. This may be potential avenues for further research and inquiry.

Keywords—PICO, 5G, mobile networks, security, smart health.

Acknowledgements

First and foremost, I thank God for making it possible that I complete my studies. I would like to acknowledge my supervisor, Dr Bessie Malila who wholeheartedly offered to be my main supervisor after the passing of our esteemed dearest Professor Tania Douglass. I would like to thank Dr Bessie who, throughout this entire process remained patient and kind and has provided me with consistent assistance even under the current unpleasant time of COVID 19. Thanks to all academics who have been of support to me in various ways, Dr Jill Fortuin Abrahams, Dr Fatimah Salie and Dr Nailah Conrad.

I would also like to acknowledge my late parents Ndarhwa Athanase and Consilie M'chishashu in whose honour I am conducting this master's degree. Many thanks to my family who have supported me from afar, and my Fiancé Ezechiel, for his undying love and encouragement throughout this process.

Thank you.

Table of Contents

List of Tables

List of Figures

Glossary of Terms

List of Abbreviations

IoT	Internet of Things
IoMT	Internet of Medical Things
DoS	Denial of Service attack
4G	Fourth Generation Network
5G	Fifth Generation Network
MHealth	Mobile Health
PHI	Patient health information
EHR	Electronic Health Records
PICO	Problem, intervention, comparator and outcome (systematic review search strategy)
PROSPERO	International Prospective Register of Systematic Reviews
PRISMA	Preferred Reporting Items for Systematic Review and Meta-Analysis

1. Introduction and Problem Identification

Smart healthcare systems are interconnected infrastructures that comprises medical devices, health systems and services, and embedded technologies that are used to monitor patients and deliver healthcare services (Tian et al., 2019). Smart healthcare systems are set to transform healthcare, for example, through the use of applications on mobile devices equipped with sensors for collecting physiological signals and health data; providing services such as teleconsulting; delivering health information to practitioners, patients, consumers of healthcare services, and researchers; remote real-time monitoring of vital signs; and training and collaboration of healthcare workers (Jagadeeswari et al., 2018, Luna et al., 2016, Ahmed et al., 2020).

Although smart healthcare systems are set to provide tremendous opportunities to transform the healthcare sector globally, Africa and Sub-Saharan countries are still at the verge of implementing smart healthcare systems due to lack of policies and strategies to standardize the use of smart healthcare systems such as smart implants(Gaobotse et al., 2022).

To provide ample services, smart healthcare systems rely on mobile networks for their full functionality. Mobile networks therefore constitute one of the cornerstones of smart healthcare systems.

Mobile networks have experienced exponential growth over the years. From the first generation to the current fifth-generation network (5G), and they have contributed to the development of smart healthcare systems (Samaoui et al., 2015). The emerging 5G network is expected to revolutionize healthcare service delivery as compared to previous generation networks (Latif et al., 2017, Mwangama et al., 2020). This is due to the performance enhancements in 5G mobile networks which are part of the key drivers for the adoption of smart healthcare systems, and will allow the proliferation of connected healthcare services and applications. However, security and privacy of patient health information is one of the major challenges that need to be addressed before the benefits of smart healthcare systems can be fully realized. Smart healthcare systems deployed using 5G technologies will be more vulnerable to security threats due to the expected deployment of a large number of connected medical devices (Internet of medical devices) (Malila and Mutsvangwa, 2019, Mwangama et al., 2020). Therefore, certain security measures should be implemented to mitigate the security risks associated with connected health systems (Al-Janabi et al., 2017). However, the mitigation of security risks depends on the security requirements that are implemented in the smart healthcare system(Sridharan, 2010).

Security requirements for connected healthcare smart systems can be broken down into three key components, i.e., confidentiality, integrity, and availability. Confidentiality refers to the protection of data from being exposed to access by unauthorized users; data integrity refers to different measures taken to prevent changes to the content of a message and its accuracy; and availability refers to the accessibility of information by authorized users (Crosby, 2012, Tan et al., 2008, Al-Janabi et al., 2017). Furthermore, to guarantee the effectiveness of these security components, two additional features are required, namely authentication, which verifies the identity of the user, and authorization, which ensures that the user has the right to perform the tasks they wish to perform within the system (Crosby, 2012). To secure and protect sensitive medical information in connected healthcare systems, several mitigation measures have been proposed. Examples include data encryption, use of cryptographic keys and biometrics, and implementation of system-wide

frameworks based on technologies such as Blockchain and X-Road (Ramli et al., 2013, Memon and Mustafa, 2015, Malila and Mutsvangwa, 2019).

Although these security measures have shown the potential to improve the security of data in existing healthcare systems, there are still many security risks that cause vulnerabilities in smart healthcare systems due to their distributed and decentralised nature and the openness of wireless systems. These include denial of service attacks performed on servers in cloud-based storage and processing systems, reverse engineering attacks - a process by which a device is deconstructed to reverse its initial design (Imane et al., 2019), bots - a malicious software installed on mobile or medical devices for stealing medical information, eavesdropping on wireless or wired communication links and unauthorized access to data (Kumar et al., 2014). Attacks targeted at these vulnerabilities have negative physical, social, and economic effects on patients, and can potentially result in patient injury or deaths (Sridharan, 2010). For example, changes to patient data can lead to misdiagnosis hence wrong treatment interventions (Imane et al., 2019, Sridharan, 2010).

This systematic review aims to review security issues in emerging smart healthcare systems, with a focus on the security requirements, potential security risks, the measures currently being proposed to mitigate these risks, and the effectiveness of the proposed mitigation measures. The results of the study are set to inform security system designers on the best strategies for developing security mechanisms for smart healthcare systems. The results will also be useful to network operators in highlighting the potential risks to health information as it traverses mobile networks. The results will further be useful in educating departments of health in the potential risks of publicly shared health data, possible mitigation measures, and potential solutions. This study has also been presented at the H.i.P Biennial Research Symposium. This research has been peer reviewed and the paper was presented at the SATNAC conference. The presented paper is attached as appendix E.

1.1. Research Questions

The main research question that was answered in this systematic review is: what are the security issues related to the acquisition, transmission, storage and sharing of patient health data in smart healthcare systems?

The following sub-questions were addressed:

1. What are the security requirements for secure acquisition, transmission, storage and sharing of patient health data in networked smart healthcare systems?
2. What are the security risks during the acquisition, transmission, storage and sharing of patient health data in networked smart healthcare systems?
3. What solutions have been proposed in literature to mitigate these security risks?
4. How effective are the proposed security solutions?

The strategy used in this systematic review is based on the PICO, i.e., problem, intervention, comparator and outcome systematic strategy. The PICO table used for this systematic review is shown in Table 1. The problem addressed in the study was the challenges in ensuring the security and privacy of patient health data in smart healthcare systems. The intervention was the measures that have been taken to mitigate security risk in smart healthcare systems. The comparator was not

applicable because this review focused on the security measures available, and in this case no comparable solutions were considered since the concept of smart healthcare systems is an emerging one and there are therefore, no existing security solutions that have been used before. The outcome was the improvements in the security and privacy of patient health information during data acquisition on mobile and medical devices, transmission on communication systems and access in storage and processing servers.

Table 1: PICO table

Problem	Security for patient data in smart healthcare systems
Intervention	Security risks measures in smart healthcare systems
Comparator	None
Outcome	Improved smart healthcare systems for patient data in terms of security, sharing, storage and access control.

2. Literature Review

This section reviews the literature on security and privacy issues in smart healthcare systems. The literature review focuses on three main issues: (1) a description of mobile networks as a key enabler of smart healthcare systems (2) the security requirements and (3) the security solutions proposed in the literature to address each security requirement.

2.1. Mobile networks as an enabler of smart healthcare systems

Mobile networks have experienced rapid growth and remarkable performance improvements over the past decades. They have become the core element of communication between individuals across different geographical locations by enabling communication services anytime and anywhere (Samaoui et al., 2015). Mobile networks have significantly gained ground in developed countries of Europe, America and in the Pacific Rim as compared to African countries. Africa has been a straggler in the evolution of high speed data networks. This leads to closing the gap that has been opened with the use of mobile networks as compared to Europe and America(Curwen and Whalley, 2018). Mobile networks have evolved through a series of generations. The evolution from the first to the fourth generation brought a transition from voice calls to multimedia data transmission (Samaoui et al., 2015, Alquhayz et al., 2019). The fourth-generation network (4G) is a radio access system that offers high bandwidth connectivity and enables users to seamlessly access multimedia content on various communication system platforms (Alquhayz et al., 2019). Initially, 4G was meant to meet major requirements such as increased data capacity, improved internet access, and higher bandwidth, allowing mobile networks to operate ten times faster than 3G (Alquhayz et al., 2019). However, several limitations are becoming a reality in the 4G era as user demands increase. Some of the limitations include achievable data rates, high network latency, and a limited number of possible connections (Samaoui et al., 2015, Alquhayz et al., 2019). Furthermore, 4G cannot meet the anticipated performance demands of emerging technologies such as the provision of remote real-time virtual and augmented reality services, transfer of large data files required in artificial intelligence applications, and other special services such as real-time remote surgery, remote disease diagnosis or teleconsultation.

The fifth-generation of mobile networks (5G) are expected to address some of the limitations of current mobile systems. For example, they use an adaptable radio access network to offer the flexibility required in handling fluctuations in traffic demands and heterogeneous services expected in connected healthcare systems (Mwangama et al., 2020). The focus of 5G is to provide better levels of connectivity and coverage compared to previous generation networks; high speed and high-capacity data transfer and allows high-quality multimedia applications. These capabilities are key for the successful implementation of smart healthcare systems (Malila and Mutsvangwa, 2019). In Africa, 5G-enabled digital healthcare systems have the potential to positively impact health outcomes by enabling the development and deployment of state-of-the-art applications that may be useful in rural areas (Mwangama et al., 2020). 5G systems are expected to transform healthcare service delivery. However; the open nature of 5G systems creates an increased security attack surface. Securing patient health data has therefore been identified as a significant barrier to the full realization of smart healthcare systems (Malila and Mutsvangwa, 2019).

Furthermore, the 5G architecture is intended to support the communication needs of machine-to-machine and machine-to-human applications in smart health systems and this will impose high-security risks to patient health information (Arfaoui et al., 2018).

The evolution of mobile networks is illustrated in Table 2. The table illustrate the start and end dates of each mobile network generation, their primary services and download speed, as well as some of the limitations associated with each mobile generation network as they relate to smart healthcare systems.

Table 2 Evolution of mobile networks from 1G to 5G (Samaoui et al., 2015, Alquhayz et al., 2019).

Network	1G	2G	3G	4G	5G
Start and deployment	1980-1990	1990-2000	2000-2010	2010-2020	2020-2030
Download Speed	2Kbps	64Kbps	2Mbps	1Gbps	1Gbps to 10Gbps
Primary Service	Analog phone calls	Digital phone calls and messaging	Digital phone calls, messaging and data transfer, Internet	All Internet Protocol services	High-speed data transfer, high network capacity.
Main differentiator	Mobility	Secure mass adoption	Better internet access	Lower latency, faster broadband internet	Better connectivity and network coverage

Smart healthcare systems are connected to the Internet and use mobile platforms which allow them to utilize technologies such as wearable devices and Internet of Things (IoT) to dynamically connect people and provide access to health services and information related to healthcare (Tian et al., 2019). Smart healthcare can address different needs, as illustrated in Table 3, such as assisting diagnosis and treatment using technologies such as artificial intelligence, mixed reality, and surgical robots. Another example would be providing virtual assistants by using algorithms that communicate with users using techniques such as speech recognition.

Table 3 Applications of smart healthcare (Tian et al., 2019).

Smart healthcare need	Technology solution
Assisting diagnosis and treatment	The application of technologies such as artificial intelligence, mixed reality, and surgical robots.
Health management	The use of a new model of smart healthcare which focuses on patient self-management. Patient self-management puts emphasis on real-time self-monitoring of patients using wearable smart devices.
Disease prevention and risk monitoring	The use of disease risk prediction models that allow data collection using wearable devices and smartphone-based applications which send the collected data to the cloud communication networks.
Virtual assistants	Virtual assistants are algorithms that communicate with users using techniques such as speech recognition; they obtain information from sources, then respond according to the user's needs. In healthcare, users may be patients or healthcare professionals.
Smart hospitals	Smart hospitals rely on the IoT to connect intelligent buildings, digital devices, medical devices and personnel.

2.2. Security requirements in smart healthcare system

The security requirements for connected smart healthcare systems are confidentiality, integrity, and availability of data. In addition to these, authentication is required for verifying credentials of users (in the case of human to machine interaction) or machines (in the case of a machine-to-machine interactions) before they can access services or systems. Furthermore, authorization is a security requirement aimed at ensuring that users only gain access to resources or information that they are allowed to access (Tan et al., 2008, Crosby, 2012, Chan and Hong, 2016, Tan, 2018, Arfaoui et al., 2018). A detailed explanation of these requirements is given in table 4 below.

Table 4 Security requirements in smart healthcare system

Security requirement	Definition
Confidentiality	Confidentiality means that the data should be accessible only to intended users. Unauthorized access to data can have a negative social and economic impact. Confidentiality is the core element in smart healthcare systems as it ensures that patient's data is solely accessible to authorized healthcare professionals (Arfaoui et al., 2018).
Integrity	Integrity relates to the trustworthiness, correctness, and completeness of the health data and is addressed by two mechanisms: detective mechanisms intended for detection of unauthorized modification of data, and preventative mechanisms which are intended to prevent unauthorized modification. In healthcare systems, Integrity is important because modification to patient data can lead to inappropriate treatment, misdiagnosis, and a threat to patients' health (Crosby, 2012).
Availability	Availability is the degree to which data is accessible to authorized users and is a critical element of the healthcare system. (Tan et al., 2008).
Authorization	Authorization is the process of ensuring that appropriate access privileges are given to authorized users (Tan et al., 2008). In health systems, appropriate authorization ensures a seamless flow of activities and improves the quality of service (Chan & Hong, 2016).
Authentication	Authentication is based on proof. The system must ensure that the user or device is who they say or claim (in the case of a device) they are. Message authentication ensures that the message that is being delivered is the same as that which was created (Crosby, 2012; Tan, 2018).

2.3. Security risks in smart healthcare systems

This section describes possible security risks in smart healthcare system. Figure 1 illustrates the different forms of security attacks that can compromise the confidentiality, integrity and availability security requirements of smart healthcare systems (5GAmericas, 2019, Imane et al., 2019, Ferrag et al., 2017).

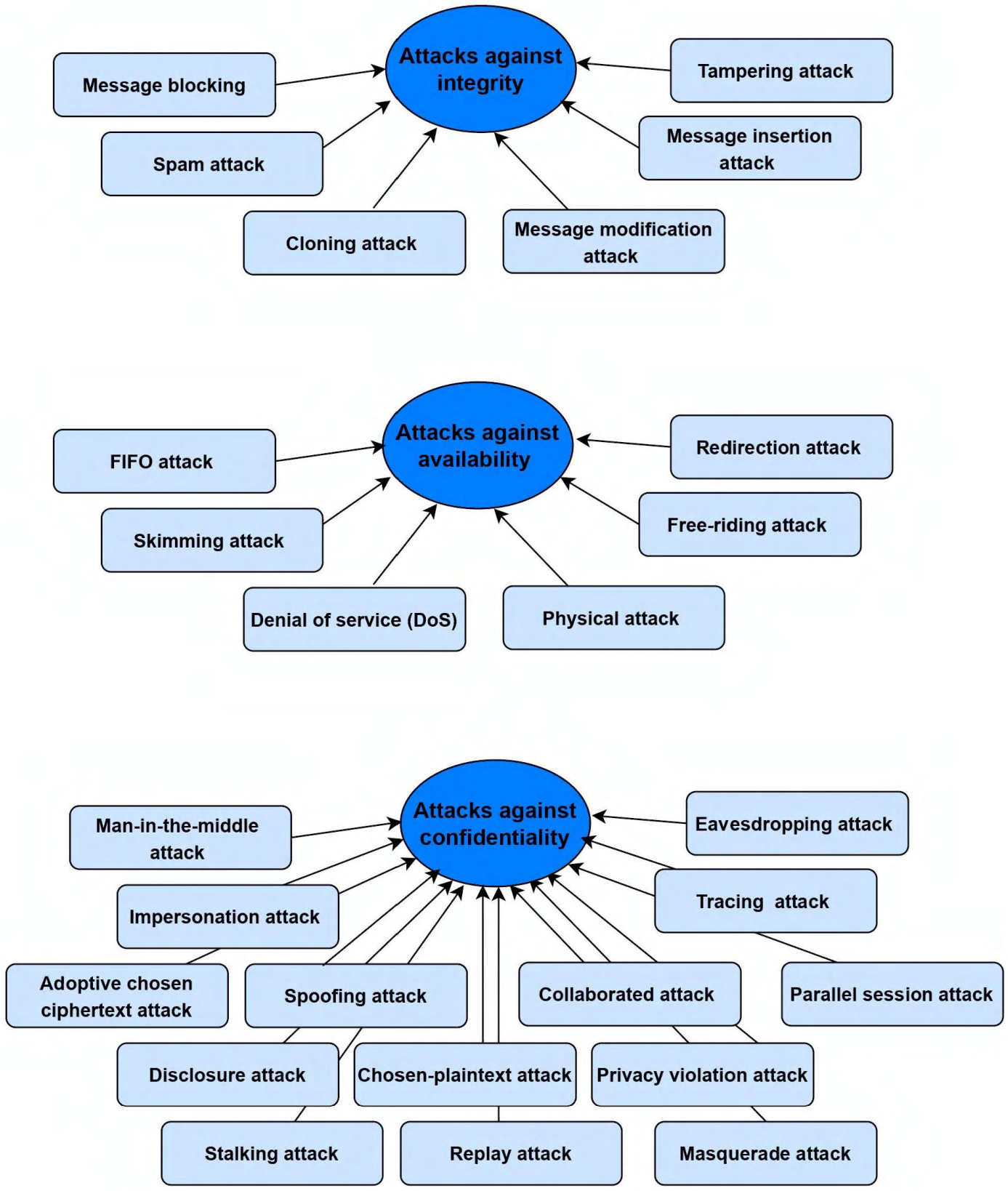

Figure 1 System security attacks (Ferrag et al., 2017, Imane et al., 2019)

These security risks are described as follows:

Security risk to confidentiality

The privacy and confidentiality of data may be threatened through several types of attack, namely unauthorized access to data, network, or system (Kumar et al., 2014). Violations of data confidentiality occur when an attacker accesses the system or the network without being noticed and steals data with the intention to modify or misuse the data (Imane et al., 2019). In smart healthcare systems, this can result in physical, emotional, or financial harm to the patient (Kumar and Lee, 2012, Kumar et al., 2014).

Security risk to availability

Threats to the availability of data may occur through several types of attack (Imane et al., 2019). Denial of service (DoS) is an attack in which a malicious actor aims to render a computer or other devices unavailable to its intended users by interrupting the device's normal functioning. When a DoS attack occurs in a healthcare system, it results in healthcare workers being unable to access health data that may be critical for disease diagnosis or treatment decisions by clinicians. Inability to timely access to patient data can result in disease progression, late intervention, or patient death (Sridharan, 2010, Imane et al., 2019).

Security risk to integrity

Threats to the integrity of data include attacks such as message modification, tampering or message insertion (Imane et al., 2019). These attacks enable the intruder to modify healthcare data and feed, replace or insert incorrect data within the healthcare data set. Consequently, incorrect data could lead to misdiagnosis which may affect a patients health and the types of intervention (Sridharan, 2010, Imane et al., 2019).

2.4. Measures to mitigate security risks in smart healthcare systems

When implementing smart healthcare systems using 5G networks, several security measures are required to mitigate the effects of security risks (Alquhayz et al., 2019). Below are some of the measures that have been proposed and implemented to mitigate the effects of security risks in smart healthcare systems.

Biometrics are body measurements and calculations related to human characteristics. Biometric authentication (or realistic authentication) is used as a form of user identification and access control. It is also used to identify individuals in groups that are under surveillance (Ramli et al., 2013). Biometrics have been proposed to secure health data in wireless body area networks due to their reduced computational complexity and better power efficiency compared to other security mechanisms (Al-Janabi et al., 2017). Some of the limitations of this security measure are the issue of cost, in order to acquire advance security system, and the issue of data breaches by attackers which may cause threat to biometric data as it is irreplaceable and sensitive (Agrafioti et al., 2011).

Data Encryption is a widely used method for ensuring data confidentiality and integrity. Several research has been conducted in the use of data encryption techniques in ensuring the confidentiality of data in smart healthcare systems. Researchers address the resource limitations of some of the IoT systems used in smart healthcare which make it difficult to implement traditional data encryption algorithms which require a huge amount of processing and storage resources to be operational (Medileh et al., 2020, Daniel and M., 2011). An assumption made in the design of encryption algorithms is that by increasing the key-size with a higher encryption round, better security can be achieved. However, this creates problems such as an increased complexity of the algorithm, system operational overhead and resource exhaustion. This problem is more pronounced in small sensor devices used in smart healthcare systems, due to the sensor's node limited computational energy capacity, processing power, and memory space (Al-Janabi et al., 2017). There is therefore need to develop new techniques for data encryption (Gurumanapalli and Muthuluru, 2021).

X-Road is a system that enables secure communication between organizations (Freudenthal, 2015). Is a distributed technology which allows data shared among multiple systems in different geographical locations. In a distributed computing, data processing is spread though out multiple computers over a network. Therefore, X-Road is a suitable technology for securing smart healthcare systems, which also have a distributed architecture. To ensure the integrity, confidentiality, and availability of data, X-Road uses its own public key infrastructure solution, where all the service providers hold public key certificates to allow a time stamped digital signature of all queries and replies (Ansper et al., 2013). X-Road has been proposed to secure health information while in transit in mobile networks (Malila and Mutsvangwa, 2019). The technology is currently being developed to enable sharing of health data related to the COVID pandemic between countries globally (WHO, 2021). A limitation of the X-Road security infrastructure is that by design, it only protects data from the point the data leaves the local Information Technology system and enters the remote IT system. However, security at the point of data acquisition, which would be required in smart healthcare systems and occurs in local IT systems, home networks or body area networks, cannot be guaranteed. X-road addresses the risk to confidentiality and privacy violation during data transfer in distributed data system. Another limitation of X-Road is the centralised architecture which creates a single point of failure in the protected systems like smart healthcare systems. To address this limitations, researchers have proposed the integration of X-Road and Blockchain (Malila and Mutsvangwa, 2019).

Blockchain: Blockchain is a distributed database technology that upholds a continuously evolving list of records, called blocks (Memon et al., 2019). A block of information consists of hashes of the previous and current blocks, a time stamp, and the transaction record which is in the form of a cryptographic hash value. One important feature of blockchain which is beneficial to smart healthcare systems is its decentralised and distributed architecture. This allows the implementation of security mechanisms in distributed healthcare applications and services that do not rely on a centralised authority. More importantly, blockchain uses cryptographic algorithms to encrypt the data stored to ensure that only legitimate users are able to view the data, thus supporting data confidentiality and integrity (Agbo et al., 2019). Some of the limitations of blockchain technology include the management of cryptographic keys and susceptibility to denial of service attacks (Zghaibeh et al., 2020). Furthermore, there are security vulnerabilities as data during data transfer between devices in the communication networks (Malila and Mutsvangwa, 2019). In addition to the

distributed and decentralized approach of ensuring data security across distributed nodes in 5G environments, Azzaoui, et al.(2020) argue that blockchain is able to support numerous other technologies such as artificial intelligence, which allows the creation of smarter and more secure smart healthcare systems. Similarly, Singh et al. (Singh et al., 2021) argue that blockchain provides a decentralised storage which allows for previous and current blocks to link using smart contract codes, thus supporting the data availability security requirement, a limitation of X-Road, whose architecture is centralised.

2.5. Related systematic literature reviews

In this study, recent research was examined, and two studies that conducted a systematic review of security in smart healthcare systems were identified. Hameed et al. (2021) conducted a systematic review on the security and privacy of Internet of Medical Things and found that machine learning techniques have been considerably used to mitigate security issues in medical devices and body area networks. The study mainly focused on sensor anomaly detection and device authentication. Liao et al. (2020) performed a systematic review to analyse the security of IoT devices using mobile computing. Their systematic review only focussed on mobile computing, particularly smart phones, and disregarded all other IoT devices such as medical devices. The systematic literature review performed in this study focused on the security and privacy of smart healthcare systems which encompasses the internet of medical things, and address gaps that have been omitted in the previous studies including data security at the acquisition device, data transfer through the network as well as the security of data in storage devices.

3. Research Methodology

This chapter highlights procedures used to identify, select, and analyse studies included in this systematic review. A detailed explanation of the systematic review strategy used in this study is outlined in the sub-sections below. The systematic review has been registered with the International Prospective Register of Systematic Reviews (PROSPERO). The study also adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. PRISMA is an evidence-based set of items that aim to assist researchers improve the reporting of systematic reviews and meta-analyses (Moher et al., 2009). The guidelines focus on ways in which authors can ensure the complete and transparent reporting of systematic review studies (Liberati et al., 2009). Hence, this guideline was used for identification and screening of studies in this systematic review and has presented the result in a PRISMA flowchart diagram which is illustrated in Figure 2. The study is not restricted to any geographical setting. A detailed description of the PICO for this study is given in the following sections.

3.1. PICO (Problem, Intervention, Comparator and Outcome)

This study was framed using the PICO approach to present the concepts of interest (Pati and Lorusso, 2018). The comparator was not applicable because this review focused on the security measures available. Hence, In this case no comparable solutions were considered since the concept of smart healthcare systems is an emerging one and there are therefore no existing security solutions that have been used before.

3.1.1. Problem

The problem addressed in this study is how to ensure the security and privacy of patient data in smart healthcare systems. The focus was based on data security from the point of acquisition, during transmission on communication networks, while being shared among smart healthcare system users; and during storage. Data could be stored on mobile and medical devices; hospital or cloud-based servers for the purpose of disease diagnosis, monitoring or treatment of diseases.

3.1.2. Intervention

The intervention assed in this study is the security measures that have been proposed to address the problem. The interventions included security mechanisms that have been proposed to mitigate against data security breaches in smart healthcare systems. The search focused on studies that proposed end-to-end security interventions and address the security and privacy of data from the point of acquisition, while being transferred through communication networks, and being stored on hospital or cloud-based on storage devices, and during data sharing among the smart healthcare system users.

3.1.3. Outcome

The outcome is improved end-to-end data security in smart healthcare systems. Specifically, the outcomes of interest included how security risks to data confidentiality, integrity, availability, authorization, and authentication have been mitigated in smart healthcare systems, and the effectiveness of the identified solutions.

3.2. Data sources and search Strategy

The search strategy included identification of studies from different databases including Scopus, PubMed, Web of Science, Medline, CINAHL, Ebscohost and the Cochrane Library. Throughout the search, the only three databases that yielded results were Scopus, Web of science and Medline.
The search strategy design was finalised in consultation with a library expert from the University of Cape Town Health Sciences Library. Additionally, reference lists from extracted papers were examined to find relevant studies but these yielded no results. The grey literatures searched were published dissertations, research reports, and conference papers. These were also reviewed through Google search, however they yielded zero results and this led to a limited number of articles being examined for this study. The search strategy used to search Scopus database is outlined in *Table 5* below. A comprehensive search strategy result for the above-mentioned databases is attached as Appendix 1.

3.3. Study Selection

Articles extracted from the selected databases were saved in the EndNote citation manager. The study selection was done in four stages: (1) elimination of duplicate studies, (2) exclusion of studies based on title, (3) exclusion of studies based abstracts, and (4) exclusion of studies based on the full text. The author and second reviewer performed the 4th stage of the selection process to determine the eligibility of studies using a data extraction form designed for this study (see Appendix A). This stage was the final assessment for inclusion or exclusion of the studies left after stage 3 of the selection process. Only studies that addressed the problem of security in smart healthcare systems were selected for inclusion in the reporting of the systematic review. The data extraction sheet reported PICO characteristics of each study. An adjudicator was appointed to mediate over any disagreements for inclusion or exclusion of a study between the author and the second reviewer and the opinion of the adjudicator was final.

Table 5 Scopus Search Strategy studies to be assessed

Number	Description	Query	Items Found
#1	Free Text	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain	1 077 335
#2	Free Text	4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*”	57 774
#3	#1 AND #2	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*”	4 749
#4	Free Text	Health	11 313 862
#5	#3 AND #4	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*” AND Health	375
#6	Add Filter	DOCTYPE , "ar" OR "cp" OR "ch"	329
#7	Add Filter	LANGUAGE , "English"	**324**

3.4. Data Extraction

A standardized data extraction (Appendix A) form was developed by the author and second reviewer to extract data from selected articles. Data was extracted independently by these researchers and discrepancies were discussed and resolved in consultation with the third researcher. Microsoft Excel and Review Manager (RevMan) software were used for data management.
The main data extracted included:

- Author
- Full reference and Year of study
- Type of study
- Country of Study
- Type of intervention
- Type of security issue
- Type of smart device
- Type of cloud storage
- Type of outcome
- Findings/ Results

3.5. Assessing Risk of Bias

Risk of bias was assessed by evaluating whether the outcomes were defined using reliable measures (Liberati et al., 2009). The criteria developed by the International Cochrane Collaboration, such as precision, choice of outcome measures, design of included studies, and conflict of interest in the conduct of the study, were assessed (Viswanathan et al., 2017).

3.6. Data Analysis and Synthesis

This study analysed data and reported data in the form of a narrative synthesis. Details of each included study are presented and discussed in section 4 below. According to (Pati and Lorusso, 2018) a narrative systematic review, is an approach used to report systematic reviews by synthesizing findings from multiple studies using words and texts to summarise the findings.

3.7. Dealing with Missing studies

To deal with the problem of studies, authors of articles that could not be accessed on the databases were contacted and requested to provide the full text of the articles. In cases of no response from the authors, the strategy was to conclude the study with the available articles. In this case four articles could not be retrieved and there was no response from the authors.

3.8. Subgroup Analysis

Studies were clustered and analysed based on the research questions and their reported Problem, Intervention, and Outcome. The research questions were (a) what are the security requirements for secure acquisition, transmission, storage and sharing of patient health data in networked Smart Healthcare systems, (b) What are the security risks during the acquisition, transmission, storage and sharing of patient health data in networked Smart Healthcare systems, (c) What solutions have been proposed in literature to mitigate these security risks (d) How effective are the proposed security solutions.

4. Results

4.1. Study selection

The study selection process for this systematic review was guided by the PRISMA strategy. The PRISMA flowchart for the study selection is shown in Figure 2. The process of study selection was conducted with the use of the inclusion and exclusion criteria as shown in Table 5.

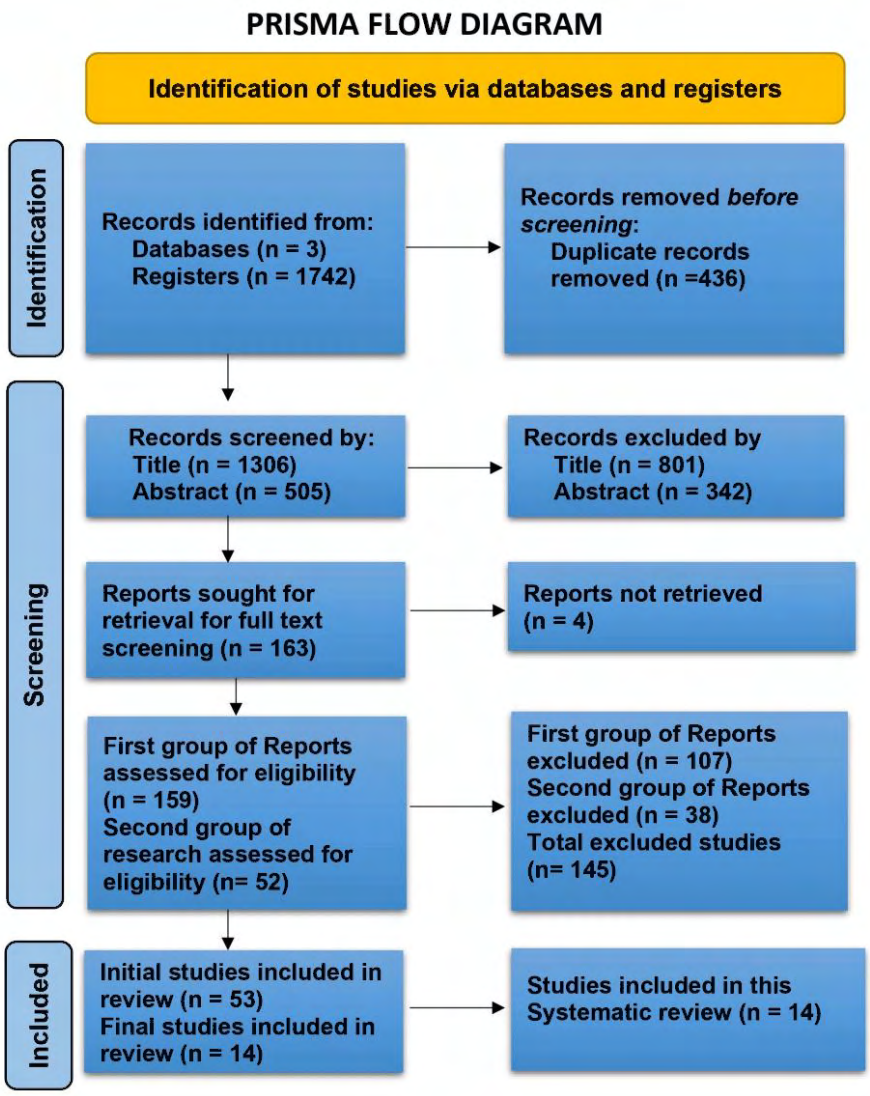

Figure 2. The PRISMA flowchart

Table 6. Inclusion and exclusion criteria table

Characteristic	Inclusion criteria	Exclusion criteria
Problem	Articles that addressed security in smart healthcare systems for patient data sharing, storage and access control.	Articles that did not focus on health related topics, security in smart healthcare systems, and end-to-end security in smart healthcare systems as well as systematic reviews, surveys, etc.
Intervention	Studies that included security mechanisms used to mitigate against data breaches in smart healthcare systems.	Articles that did not demonstrate propose or implement mechanisms for mitigating security risks at the acquisition device, security of data while being transferred through mobile networks or the security of data at the storage device are excluded.
Outcome	Studies on improved end-to-end security in smart healthcare systems for patient data sharing, storage and access control.	Studies that did not demonstrate end-to-end security in smart healthcare systems data sharing, storage and access control were excluded.

This systematic review identified a total of 1742 records through an exhaustive and comprehensive search from three electronic databases. Among these, 436 records were identified as duplicates and they were removed. Using titles and abstracts, the remaining 1306 studies were screened focusing on studies relating to the security of smart healthcare systems. Based on their titles, of the 1306 articles, 801 were excluded as they did not report on security or smart healthcare systems, leaving a total of 505 articles. These 505 were further screened by reading their abstracts and 342 articles were excluded, leaving a total of 163 articles. Of these 163, 4 records could not be found in all databases and the authors did not respond to the requests for full texts. Hence the remaining 159 were screened for eligibility based on reading the full text. Of these 159 potentially eligible studies, 107 were initially excluded; reasons for their exclusion are presented in Appendix 4, leading to 52 studies being potentially eligible for inclusion in the study.

After further analysis by both reviewers, the remaining 52 studies were reassessed, focussing on the scope of this systematic review of including only studies that reported on end-to-end security in

smart healthcare systems. As a result of this final screening, 38 studies were excluded. These excluded studies focused on security mechanisms for certain segments of smart healthcare systems, and not end-to-end security. A total of 14 studies were therefore finally included in this systematic review. A table summarising the reasons for exclusion of the excluded studies is given in Appendix 4.

4.2. Included studies overview

To demonstrate the leading countries in which researchers are focussing on the security of patient's data in smart healthcare systems, included studies were considerably examined based on their geographical settings as shown in figure 3. The figure illustrates countries in which each study was conducted. Thus, it was noted that two studies were conducted in USA, two studies in Australia, and two more in China. On the other hand, only one study was conducted in Finland, one in India, one in the United Arab Emirates, one in Northway, one in Peru, one in the Republic of Korea and finally one in South Korea.

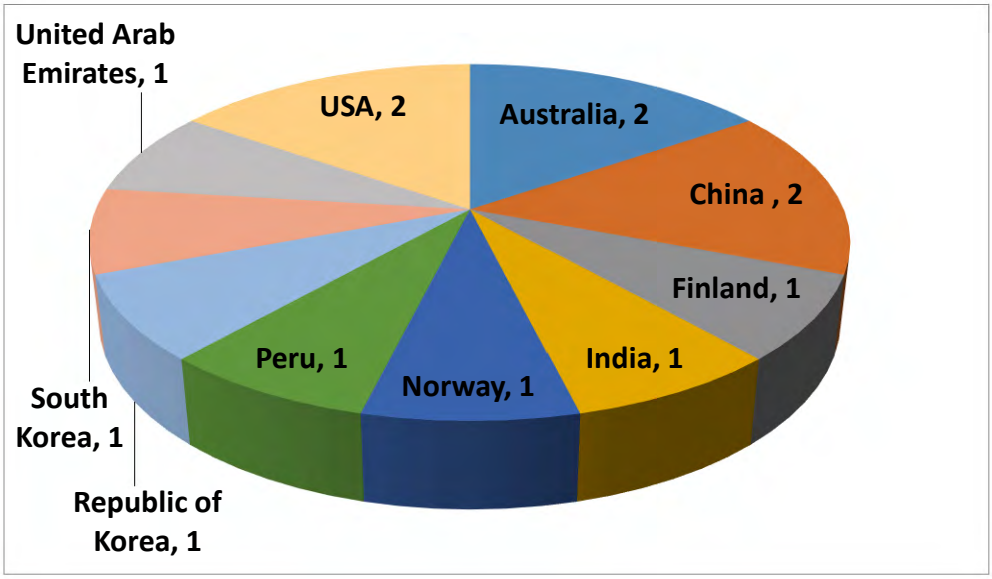

Figure 3. Included studies per country

4.3. Study Characteristics

Table 7 illustrates a list of characteristics of the included studies. These studies are referred to in the analysis and synthesis of results as they are numbered in table 6. Studies are illustrated as (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14). Firstly, these studies identified the main security requirements for smart healthcare systems as data confidentiality, integrity and availability of data within the system, with authorisation and authentication used to support these key security requirements. The main security risks reported were authentication vulnerabilities in user devices and storage servers, loss of data confidentiality due to eavesdropping in wireless communication mediums, data fabrication and message modification attacks during transmission as well as while the data is saved in databases and other storage devices. The main interventions proposed to mitigate the risks were data encryption for protecting the confidentiality and integrity of data. The use of biometric accessing devices; blockchain technology to address confidentiality, integrity, and availability of data and network slicing techniques to provide isolation of patient health data in 5G mobile systems. The reported outcomes were improvements and provision of a high level of data security in smart healthcare systems. For example, proposed encryption algorithms demonstrated better energy efficiency, and improved operational speed; reduced computational overhead, better scalability, efficiency in data processing, and better ease of deployment.

In addition, these studies reported the use of different types of medical devices, mobile devices, and patient's personal smart phones for accessing and exchanging health data. These devices used different types of storage i.e., cloud-based and local storage, as well as mHealth servers or medical servers within the healthcare systems. For instance, Afzal et al. developed a framework for secure health data transmission, using an encryption algorithm that is applied on the data before transmission (Afzal et al., 2020). The authors concluded that the issue of transmitting data through insecure networks was resolved by splitting data encryption between a client at the patient side, and a cloud server. This way a reduction in encryption time is achieved while ensuring the privacy and security of transmitted data. Thus, the client needs to be connected to the cloud, and the cloud has to be trustworthy. The encryption of data at different locations resulted in reduced encryption time and lower energy consumption at the patient side, which would consist of small medical devices with energy management issues.

Table 7: Study characteristics

Num	Authors and Year	Title	Country	Type of Smart device	Type of Storage	Type of Intervention	Type of Security Issue	Types of Outcomes
1	Belkhouja, T., A. Mohamed, A. K. Al-Ali, X. Du and M. Guizani (2017).	Light-weight encryption of wireless communication for implantable medical devices using henon chaotic system	USA	Cardiovascular and Neurological implantable Medical devices	Cloud storage	Security algorithm that creates symmetric encryption keys for medical devices	Data exchange issues using cryptographic keys	Protection of the encryption keys from theft using a developed key generator to encrypt the communication of any implantable medical device
2	Al Baqari, M. and E. Barka (2020).	Biometric-Based Blockchain EHR System (BBEHR). 2020 International Wireless Communications and Mobile Computing, IWCMC 2020	United Arab Emirates	Smart devices phones and Tablets	Database service storage	Biometric-based blockchain technology with the EHR system	Data integrity issue	The combination of a biometric-based blockchain technology and EHR system which allows the use of blockchain technology between distributed healthcare
3	Feng B et al, (2019)	Secure 5G Network Slicing for Elderly Care	Norway	Smart phones	Cloud storage	Network slicing and User authentication protocol	Data security issue	More secure patient data
4	Peña, C. A. N., A. E. G. Díaz, J. A. A. Aguirre and J. M. M. Molina (2019).	Security model to protect patient data in mHealth systems through a Blockchain network	Peru	Smart phones and PDAs Personal digital assistants	Cloud storage	Blockchain based security model used for health data processing	Data Integrity and security issues	Availability of data to authorized users, integrity to guarantee that the data has not been modified and authentication to verify the user's identity

5	Shen, B., J. Guo and Y. Yang (2019).	MedChain: Efficient healthcare data sharing via blockchain	China	Medical devices and sensors	Healthcare database	Data sharing framework that uses blockchain technology to overcome efficiency issues	Data sharing and efficiency issues	A secure and efficient healthcare system that analyzes the system performance compared to existing blockchain-based solutions in terms of communication and storage overhead
6	Liang, X., J. Zhao, S. Shetty, J. Liu and D. Li (2018).	Integrating blockchain for data sharing and collaboration in mobile healthcare applications.	China	Smart phones	Cloud storage	Blockchain based data sharing solution	Data Integrity and privacy in personal health devices	A mobile application that collects data from wearable devices and transfers it to the cloud
7	Nguyen, D. C., P. N. Pathirana, M. Ding and A. Seneviratne (2019).	Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems	Australia	Mobile devices	Cloud storage	A decentralized data sharing platform	Data sharing issues, Network security and Data privacy issues	A trustworthy access control mechanism is achieved with the use of smart contracts to achieve security of EHR amongst patients and healthcare providers
8	Afzal, I., S. A. Parah, N. N. Hurrah and O. Y. Song (2020).	Secure patient data transmission on resource constrained platform	South Korea	Medical devices and smart phones	Cloud storage	Encryption based data transmission method	Data Transmission and Network security issues	Development of a new framework for secure health data transmission using the encryption algorithm applied on the data before transmission
9	Moosavi (2015)	Session resumption-based end-to-end security for healthcare internet-of-things	Finland	Medical devices and smart phones	Cloud storage	Security protocol for a remote patient monitoring prototype	End-to-end security issues	Proposed scheme fulfills the requirements for end-to-end security for IoT based smart healthcare system
10	Choi, J., C. Choi, S. Kim and H. Ko (2019).	Medical information protection frameworks for smart healthcare based on IoT.	Republic of Korea	Smart medical devices and Sensors	Medical Servers	Security model for medical information protection framework for IoT based systems	Network traffic control issues	The outcome is a medical information protection framework that provides system security to smart healthcare systems

11	Atat, R., L. Liu, J. Ashdown, M. J. Medley, J. D. Matyjas and Y. Yi (2018).	A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems	USA	Smart phones and Sensors Medical devices	MHealth servers	Three-tier hierarchical m-health system architecture with a physical layer security scheme for data privacy	Privacy and security issues	A secure data transmission is achieved through analysis of two strategies of mobile device transmits. First transmission to the nearest neighbor device and second to the furthest neighbor device.
12	Huang, H., T. Gong, N. Ye, R. Wang and Y. Dou (2017).	Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System	China	Wearable sensors medical devices	Cloud storage	A healthcare system framework for data collection, transmission and storage using a security gateway	Privacy and security issues in Smart healthcare systems	A secure, private and improved performance healthcare system
13	Alex, S., D. P. Pattathil and D. K. Jagalchandran (2020)	SPCOR: A secure and privacy-preserving protocol for mobile-healthcare emergency to reap computing opportunities at remote and nearby	India	Smart phones	Local storage/ Phone memory	Protocol for privacy-preservation	Data Privacy issues in Mobile health	A highly reliable protocol that provides user privacy for Patient Health information (PHI) processing and transmission in mobile healthcare networks.
14	Rathnayake, R. M. P. H. K., M. S. Karunarathne, N. S. Nafi and M. A. Gregory (2019).	Cloud Enabled Solution for Privacy Concerns in Internet of Medical Things.	Australia	Mobile devices and medical devices	Cloud storage	A cloud-based encryption architecture	Security issues in internet of medical things	A cloud-based architecture which allows mitigation of security, privacy, integrity, storage and processing power challenges in a healthcare management system.

4.4. Analysis and Synthesis of results

This section presents an analysis of the 14 included studies in terms of the PICO analysis and research questions.

4.4.1. PICO Analysis

The association between the problem, intervention and the outcome was examined in the 14 included studies, and reported and discussed as such below

(a) Analysis of stated security problems

The included studies as described in Table 6; reported the problem relating to the security of patient's health information in smart healthcare systems. These studies are presented based on their similarities in reporting the problem. The authors reported that the lack of security and privacy of patient's health information in smart healthcare systems may cause threats such as eavesdropping, data fabrication and privacy violation threats which have the potential to cause harm to the system, the patient and the data. Studies also reported security problems during data sharing, exchange and transmission over communication networks; Issues of data integrity and privacy; end-to-end security issues and access control issues in electronic health records (EHR) integrated into connected medical IoT. Likewise, studies reported the issues of network security and traffic control when transferring data over the network, from the acquisition point to the storage device. Also, studies reported issues of data integrity and privacy in EHRs; which may result in the vulnerability of electronic health data due to modification when in storage systems on the devices or servers which may create security risks in smart healthcare systems. One of the key problems reported in all the studies is that most medical devices are vulnerable to security attacks due to their resource constrained nature and limited battery life which limit the security mechanisms that can be implemented in these devices (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14). Therefore, to effectively prevent these security problems, there is a need to explore the proposed security interventions.

(b) Analysis of interventions

Studies were further analysed based on the reported interventions. Some of the proposed interventions to mitigate security risks in IoT-based medical devices, include a protocol for privacy-preservation (13); a healthcare system framework for data collection, transmission and storage (12); a three-tier hierarchical m-health system architecture with a physical layer security scheme for data privacy (11); a cloud-based encryption architecture (14); end-to-end security protocol to assist in remote patient monitoring prototype (9); and a network slicing and user authentication protocol (3).

For the same purpose, different interventions have been proposed by studies that reported the problem of ensuring the data integrity and privacy of patient health data. These are an architecture which combines biometric-based blockchain technology with the EHR system (2); a blockchain based security model to protect electronic health data (4); and a blockchain-based data sharing solution for collaboration and data security in healthcare applications (6).

In other studies, authors propose interventions that includes a security algorithm that creates symmetric encryption keys for medical devices (1); A data sharing framework that uses blockchain technology in order to overcome efficiency issues in healthcare systems (5); A decentralized data sharing platform to secure EHR (7); an encryption-based data transmission method for secure patient data transmission (8); and a security model for IoT based systems to protect medical information (10). This allows the healthcare systems to benefit from these interventions and provide better outcomes.

(c) Analysis of outcomes

Studies were further analysed based on the reported outcomes. The analysis showed that certain studies achieved similar types of outcomes. In pioneer work carried out by (3, 9, 11, 12, 13, and 14) authors demonstrate a focus on end-to-end security as well as integration of access control in EHR into IoT-based medical devices and report a similar outcome, which is the provision of higher security level. Furthermore, other studies (2, 4 and 6) demonstrates a focus on data integrity and privacy of EHR and report outcomes such as the use of emerging security models such as blockchain technology in EHR, which allow patients to utilize their biometrics in blockchain-based EHR to access their electronic health data. This intervention ensures availability of data to authorized users, data integrity and user authentication. Blockchain therefore addresses the key security requirements in smart healthcare systems, i.e. confidentiality, integrity and availability.

Lastly, other studies demonstrated a focus on secure data sharing, exchange and transmission over the network in smart healthcare systems (1, 5, 7, 8 and 10). These studies reported similar outcomes such as secure encryption techniques for protection of the encryption keys from theft using a developed key generator. This key is used to encrypt the communication of any implantable medical device, and this provides a secure and efficient healthcare system. The authors also reported that a trustworthy access control mechanism in Blockchain-based systems can be achieved through the use of smart contracts in EHR when sharing data between patients and healthcare services providers.

4.4.2. Analysis based on research questions

The studies were classified into different subsections and analysed while trying to answer the research questions. This section presents an analysis of the studies based on the research questions.

a) What are the security requirements for networked Smart Healthcare systems?

This question intended to provide a solution towards identifying different security requirements that are relevant for the full functionality of smart healthcare systems. The included studies reported the same security requirements i.e. confidentiality, integrity, availability, authorisation and authentication. These security requirements guide innovators when designing and implementing security measures that can provide robustness against data breaches.

Some examples of implemented security measures to meet the confidentiality security requirement were user registration, login and authentication to verify the user's identity thus ensuring that only authorised users have access to the system (3, 9, 11, 12, 13 and 14). In some of the proposed solutions (1, 5, 7, 8 and 10); the system needed to verify and validate the collected raw data and compare it to encrypted data stored in the cloud. In addition to that, the system had to follow some security procedures such as a mutual authentication between users and sensors according to secret keys generated to ensure the security, integrity and accessibility of data in the system. Other studies have demonstrated that through the implementation of authentication schemes, several security features are enabled between patients, devices and healthcare providers to allow resilience to possible attacks (2, 4 and 6). It is therefore crucial that a healthcare system meets these security requirements to avoid potential security risks.

b) What are the security risks in networked Smart Healthcare systems?

This question was intended to identify reported security risks which could potentially result in the violation of the security of patient data. The main security risk reported by several studies is the risk to confidentiality of data. These included eavesdropping in wireless communication mediums, and impersonation attacks. Reported risks to the integrity of data included data modification or replacement with incorrect data. Denial of service attack was reported as a security risk to data availability, integrity and privacy (2, 3, 4, 6, 9, 11, 12, 13 and 14). Other reported risks included authentication vulnerabilities and malware attacks (1, 5, 7, 8, and 10). Attacks on the system could lead to disastrous cases such as data modification through replacement with incorrect data. These risks are detrimental to smart healthcare systems by making patient data prone to attacks. This creates the need for measures to mitigate these security risks.

c) What solutions have been proposed in literature to mitigate these security risks?

To answer this question, this section describes the different mitigation measures reported in the included studies.

A home-based Elderly Care Solution is proposed in (3), which uses 5G mobile networks slicing to provide an inherent secure connection between healthcare providers and patients. In (9), a session redemption-based end-to-end security scheme is proposed. This scheme is achieved by enabling certificate-based handshake between end-users and smart gateways which allows direct communication between the two to avoid data vulnerability. A three-tier hierarchical mHealth system with a physical layer security scheme is proposed in (11) consisting of a sensor network for collection of patient's vital signs, a mobile computing network for routing the data and a back-end network tier to analyse and provide patient's medical data security and privacy. Additionally, Authors in (12) proposed a healthcare system framework that uses smart gateways in wireless network infrastructure for secure data collection, data storage and data transmission. This is achieved through the use of a key distribution scheme and an encryption matrix to securely transmit data through the system and further perform an analysis stimulation to ensure the security of data. A secure and privacy-preserving protocol for health data processing in mobile healthcare network is proposed for patient's data privacy (13). This is achieved through the use of 4G network base stations which allows an opportunity to minimize privacy disclose of the user when accessing patient's data either nearby or remotely. Also, a cloud-based encryption architecture which uses three types of encryption techniques, i.e. Advanced data encryption, attribute-based encryption and proven data possession is proposed in (14). Blockchain technology is proposed to ensure data integrity and privacy of EHRs by incorporating biometric techniques for data access (2).

Another work carried out in (6), proposed a user centric data sharing solution that uses blockchain technology to protect patient's data. This is achieved through synchronization of data to the cloud which enables easy data sharing but also allows an enhancement of identity management and data accessibility within the system to preserve its privacy. Likewise, in (4) authors propose a security model that uses blockchain technology to provide the security of data. This is achieved by the fact that all transactions in the system are protected by a cryptographic generated algorithm that uses blockchain to provide security of the collected data. Additionally, in (1), a symmetric encryption technique is proposed for encryption of wireless communication of medical devices by avoiding wireless key exchange. This is achieved by using the developed key generator to encrypt the communication of any implantable medical device. An efficient data sharing scheme is proposed (MedChain). This Scheme uses block chain technology, peer-to-peer network and digests chain to overcome efficiency issues (5). Then, in (7) proposed a secure data sharing scheme that uses smart contracts to secure Electronic health records. This data sharing scheme uses a trustworthy decentralized access control mechanism in order to achieve security of EHR amongst patients and healthcare providers. Also, in (8) a secure data transmission framework is proposed. This framework uses a complex encryption to transmit healthcare related data over the network. The encryption is done on two levels namely: strong (chaotic) encryption to ensure data integrity at the system administrator level and bitplane encryption which is done at the user level on the entire data set. Finally, in (10) an IoT-based smart healthcare security model framework is proposed to help design security areas for IoT services. This s achieved by the ability of the framework to allow expansion of the IoT medical system and provide security to medical information. The framework

also allow mutual authentication between smart healthcare systems and medical devices and therefore contributing towards construction of a safe and secure IoT environment.

d) How effective are the security solutions?

Referring to the proposed security solution of an end-to-end security as well as access control in EHR integrated into IoT, the proposed security framework was shown to be effective by isolating the health traffic from general traffic. This was achieved through the implementation of a healthcare network slice reserved for caregivers and healthcare personnel that provides connectivity and smart home network slice to the elderly home (3). Moreover, the end-to-end security scheme proposed in (9) showed 97% more energy efficiency and was 10% faster than certificate-based and symmetric-based solutions. The authors also reported that their proposed session redemption approach consumes 2.2 times and 2.9 times less RAM and ROM compared as compared to certificate-based and symmetric-based solutions. The effectiveness of a smart healthcare system was demonstrated in (11) by showing that the transmitter is able to communicate with its neighbours with a higher average secrecy probability without the need of secure protocols such as RF Fingerprinting found in other cyber-physical systems. The transmitter was able to extend its secure communication range by learning user's behaviour and trustworthiness. Also, being equipped with information on possible eavesdropping attack, the system is able to better perform in terms of secrecy and latency. In (12), the effectiveness of the security proposed in the healthcare system framework is reported in three ways, i.e. the storage cost is very low, the network connectivity is approximately at a 100% and the security analysis shows that the encryption scheme uses a matrix permutation technique to allow only the source to see the plaintext data. Therefore, it allows direct communication between user's mobile and embedded medical devices in wireless sensor network-based smart healthcare systems and enforces privacy preserving strategies and attains satisfactory performance. In (13), the proposed solution was reported to be more effective than an existing study - Meshram's scheme - described in the study in terms of consumed resource and computational energy. Authors reported that as the number of system users increased, the resources required by the user's smart devices decreased. Also, the solution proposed in (14) was shown to be more effective in checking and validating the correctness of encrypted data stored in the system. This is done by comparing the encrypted data stored in the cloud to the raw data input using advanced encryption methods. The authors concluded that this has resulted in an increase in data security, privacy and integrity; security and lower processing power.

Additionally, in (2), the study compared the use of secret and private keys to the use of biometric based mechanism such as fingerprints. The proposed mechanism resulted in the reduction in computational overhead required from patient's devices, compared to the use of secret keys. The proposed use of fingerprints was also shown to be better at providing audit logs of system activities. A security model proposed in (4) was shown to be effective by evaluating the system performance based on its scalability and efficiency in data processing as compared to other general data security schemes which have an overall average response time of 5 to 10 seconds per 10 000 user requests. The results showed an average response time of 4.27 seconds for 10 to 10 000 user requests. An average response time of 4.13 seconds per 10 000 user access grant and 2.35 seconds response time user access denial. Then in (6), the effectiveness of the proposed solution is measured by its performance in terms of computation

complexity as compared to other systems for medical data sharing. This blockchain based data sharing solution is reported to be scalable and efficient as its focuses on data validation and data integrity.

Furthermore, the work carried in (1); reported that the proposed security framework is shown to be effective by analysing and testing the random key generation. The key generation is tested based on two points. Namely, the stop-time in the system which is unknown to the adversary, and the number of iterations needed to produce the key. This leads to obtaining different key values resulting to a drastic sequence change of the generated key. Authors demonstrated that the security and randomness in the generated keys is achieved by using the proposed encryption technique. Hence the security of the encrypted message that is communicated between devices is achieved. (5) Showed how the proposed scheme MedChain was effective by analysing the system performance compared to existing blockchain-based solutions in terms of communication and storage overhead (5). The results show that in terms of the communication overhead in data access this approach facilitates integrity check in data access since it encodes the digest of data stream into a digest chain from blockchain and this allows validation of data integrity. Similarly, in terms of storage overhead, existing schemes stores all the data on the blockchain. However, for MedChain only stores the fingerprints and the rest of the data is stored on the directory servers which are mutable and the data can be removed from the servers only when the session is revoked. Hence MedChain guarantees less storage overhead.

Additionally, in (7) the decentralized data sharing platform proposed is shown to be effective by the author's performance analysis. Authors discuss that the proposed system is designed with its ability to provide flexibility as it is deployed on mobile platform and can be accessible to any authorize user with a smartphone. Additionally, authors measure the effectiveness of this system by its ability to provide high level of availability of health data anytime anywhere. They conclude that it uses a decentralized storage system which avoids single point of failure and also guarantees high security of data, integrity and privacy with the use of blockchain and smart contracts. (8) Measure the effectiveness by analysing the two-level encryption framework (Strong encryption done on the cloud and a light weight encryption done by the user) is shown to be effective by encrypting the whole image before sending it to the cloud, rather than the encryption of a portion of the image. This way, a lesser encryption time is achieved as compared to previous scheme such as the Saijjad scheme. To measure the effectiveness of the proposed framework in comparison to the Saijjad scheme, values of the encrypted data such as (Size of the compressed image, Pick signal ration, similarity index between old and new image and the number of changing pixel rate NPCR) should be as low as possible. Authors concluded that smaller values on the encrypted data was achieved, For example, I the case of medical image 1, Image dimensions were 256x256, when encrypting with the Saijjad scheme, the NPCR was 0.5784 and the proposed method yield the NCPCR of 0.6404. This method allows the preservation of the authenticity of the image as well as a lower encryption time, thus validating the effectiveness of the proposed encryption scheme. Finally, in (10), the proposed security framework is shown to be effective by comparing the CPU and Memory performance with variation in the number of hosts in a network. The test results show that when the number of hosts is small, the CPU and Memory usage is high. However, as the number of hosts increases, the CPU and Memory usage does not increase linearly, but shows a small increase. This illustrated in the graph as follows: for memory usage, single system usage for 3 hosts is 12% and 11%; and for 8 hosts and 30% for 22% for distributed system. For CPU usage the figures are 6% and 7.8% for 3 hosts and 14% and 10% for 8 hosts.

5. Discussions

This section discusses the findings while trying to provide an answer to the main research question: what are the security issues related to the acquisition, transmission, storage and sharing of patient health data in Smart Healthcare systems?

While trying to answer the above question, the identified articles at the initial search for this review were 1742. However only 14 studies were included in the review. The Included studies were classified as articles, conference proceedings, journals and chapters in books. Among these studies, 2 of the studies were implemented in USA, 2 in China, 2 in Australia and other countries around the globe such as South Korea, India, Peru, Norway, United of Korea, Finland and United Arab Emirate had 1 study each. Although Africa as a continent has undergone major changes over the years, there is need of improvement in order for Africa to fully embrace this emerging area of smart healthcare (Curwen and Whalley, 2018).

The problem investigated in this study is the privacy and security issues of patient health information in smart healthcare systems during acquisition, transmission, sharing, storage, and access of data by patients and healthcare professionals. Researchers argue that these issues are a threat to the healthcare system as a whole (Abiramy and Sudha, 2019, El Zouka, 2017, Coppolino et al., 2019). Likewise, there is an emphasis in the literature which suggests that security issues such as failure to authenticate patients, healthcare professionals or data; puts the entire system at risk and therefore creates an easy entry for malicious attacks (Abiramy and Sudha, 2019, Fan et al., 2016, Alzahrani et al., 2020). The included studies reported the main security requirements as confidentiality, integrity, and availability, data access issues as well as network security or data transfer issues. These requirements are the core foundation to a robust and secure system (Acharya et al., 2015). Furthermore, this review attempted to highlight potential security risks in emerging smart healthcare systems. These were risks to the confidentiality, availability and integrity of data. The healthcare system is prone to these risks which could cause drastic harm to patient's data (Peña et al., 2019). To mitigate these security risks, measure such as encryption of data, the use of biometrics to identify and authenticate users, and the use of blockchain technology to protect patient's information were proposed. These proposed mechanisms demonstrated their effectiveness in addressing the security issues in smart healthcare systems and providing end-to-end security of data. For example, by using the biometrics (fingerprints) mechanism for access control on the EHR, this eliminates the risk of permanent loss of identity and access control to EHRs and further assures patients data privacy (13). Another example is demonstrated through the use of a physical layer security scheme that was proposed for mobile computing tier in m-Health, where patients medical data was transferred with secrecy and delay constraints was achieved (11). Also, by using MedChain, users exchange data through the blockchain technology which allows transaction of data without the need for a decentralized third party. This scheme is proven to provide efficient data sharing without any security compromise (5).

Based on the analysis conducted, the included articles described smart healthcare systems and identified the security requirements, security risks and solutions to mitigate the risks. Each study also explained the effectiveness of their proposed security solution. However, it was evident that some studies briefly reported the effectiveness of their proposed solution and this was considered poor reporting. Of the 14 studies included in the final selection, most of them focused on detecting security risks that have potential to cause harm to user authorization, data authentication, confidentiality, integrity and availability. However, while doing the study selection, it was evident that most of the excluded studies only focussed on user authorisation and authentication, and not data security in the system as a whole. The proposed mitigation measures within the included studies were: the use of biometrics, data encryption, blockchain technology, and multi-factor authentication. Studies showed that these proposed measures have the potential to transform the security of smart healthcare systems and therefore provide the security of data from the point of acquisition, while the data is being transferred through mobile networks, and during data storage.

5.1. Limitations

The limitation of this research is that it was carried out based on a few selected online databases (3) namely Scopus, Medline and Web of Science due to other databases yielding result of 0 studies after the search queries were performed. Additionally, 4 articles could not be retrieved for full text analysis.

This was considered to be a selection bias which occurs when a selected sample is not entirely represented (Jahan et al., 2016). Based on the titles and abstracts of the 4 missing articles, it was evident that if the full texts were available, they could have been included in the study. Therefore, this systematic review would have had 18 articles to be included instead of 14 and this could potentially add more information to the study. Researchers argue that they have experienced similar limitations on study selection when conducting a narrative systematic review (Jahan et al., 2016, Pahlevan-Sharif et al., 2019).

6. Conclusion

In this study, a comprehensive systematic review on the security issues in smart healthcare systems was conducted. The designated research question was answered by examining reported security risks in emerging smart healthcare systems such as data modification, authentication vulnerabilities and loss of data confidentiality. Likewise, the ability of mitigation measures to protect sensitive medical information were examined which include blockchain technology to address data confidentiality, integrity and availability and providing isolation of patient health data in 5G mobile systems; data encryption for protecting the confidentiality and integrity of data and the use of biometric for accessing devices. Consequently, studies reported on improvements and provision of a high level of data security in smart healthcare systems. For example, proposed encryption algorithms demonstrated better energy efficiency, and improved operational speed; reduced computational overhead, achieved a better scalability and efficiency in data processing, as well as better ease of deployment.

Therefore, the proposed risk measures are crucial in order for the healthcare system to resist attacks and provide data security and privacy in smart healthcare systems. These measures have reported the potential to transform the security of smart healthcare systems and therefore to providing security of data from the point of acquisition, while being transferred through mobile networks, and during storage. Based on the above analysis and results, it is evident that the issue of securing data throughout its process from the acquisition, while being transferred through the network as well as at the storage has been resolved by adherence to security mechanisms. The results of the study are set to inform security system designers on the best approaches and policies for developing security mechanisms in smart healthcare systems. This can be achieved through consideration of the performance evaluations of proposed security mechanisms to achieve a better decision making and policy implementation. The results may also be useful to network operators by avoiding potential risks to health information as it traverses mobile networks. The results could further be useful to conscientise departments of health in the potential risks of publicly shared health data, possible mitigation measures, and potential solutions. Hence, this will positively impact the security for smart healthcare system as whole.

All the included studies reported the effectiveness of their mitigation measures against security risks in smart healthcare systems. These studies focused on the protection of patent's data from attackers who may cause harm. However, there is lack of studies that focuses on protection data in cases where the intruder has already accessed the system. This leaves a gap for researchers to consider exploring the area of security of healthcare systems by detecting the attacker who has already gained access into the system as well as the protection of data after intrusion. Recommendations for future research and open research issues include the need for future studies to focus on intrusion detection within smart healthcare systems.

7. References

ABIRAMY, N. V. & SUDHA, S. V. 2019. A secure and lightweight authentication protocol for multiple layers in wireless body area network. *Smart Innovation, Systems and Technologies.*

ACHARYA, S., EHRENREICH, B. & MARCINIAK, J. OWASP inspired mobile security. Proceedings - 2015 IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2015, 2015. 782-784.

AFZAL, I., PARAH, S. A., HURRAH, N. N. & SONG, O. Y. 2020. Secure patient data transmission on resource constrained platform. *Multimedia Tools and Applications*.

AGBO, C. C., MAHMOUD, Q. H. & EKLUND, J. M. 2019. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare (Basel),* 7(2)**,** 7.

AGRAFIOTI, F., BUI, F. M. & HATZINAKOS, D. 2011. Medical biometrics in mobile health monitoring. *Security and Communication Networks,* 4**,** 525-539.

AHMED, I., KARVONEN, H., KUMPUNIEMI, T. & KATZ, M. 2020. Wireless Communications for the Hospital of the Future: Requirements, Challenges and Solutions. *International Journal of Wireless Information Networks,* 27**,** 4-17.

AL-JANABI, S., AL-SHOURBAJI, I., SHOJAFAR, M. & SHAMSHIRBAND, S. 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal,* 18(2)**,** 113-122.

ALQUHAYZ, H., ALALWAN, N., ALZAHRANI, A. I., AL-BAYATTI, A. H., SHARIF, M. S. & KHATTAK, H. A. 2019. Policy-Based Security Management System for 5G Heterogeneous Networks. *Wireless Communications and Mobile Computing,* 1(4582391)**,** 14.

ALZAHRANI, B. A., CHAUDHRY, S. A., BARNAWI, A., AL-BARAKATI, A. & ALSHARIF, M. H. 2020. A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks. *Symmetry,* 12.

ANSPER, A., BULDAS, A., FREUDENTHAL, M. & WILLEMSON, J. 2013. High-performance qualified digital signatures for X-road. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).*

ARFAOUI, G., BISSON, P., BLOM, R., BORGAONKAR, R., ENGLUND, H., FELIX, E., KLAEDTKE, F., NAKARMI, P. K., NASLUND, M., O'HANLON, P., PAPAY, J., SUOMALAINEN, J., SURRIDGE, M., WARY, J. P. & ZAHARIEV, A. 2018. A Security Architecture for 5G Networks. *IEEE Access,* 6(1)**,** 22466-22479.

CHAN, J. H. & HONG, J. L. 2016. Mobile security and its application. *International Journal of Security and its Applications,* 10**,** 89-106.

COPPOLINO, L., D'ANTONIO, S., ROMANO, L., SGAGLIONE, L., MAGLIULO, M. & PACELLI, R. Protecting critical business processes of smart hospitals from cyber attacks. Proceedings - 15th International Conference on Signal Image Technology and Internet Based Systems, SISITS 2019, 2019. 363-367.

CROSBY, G. 2012. Wireless Body Area Networks for Healthcare: A Survey. *International Journal of Ad hoc, Sensor & Ubiquitous Computing,* 3(3)**,** 1-26.

CURWEN, P. & WHALLEY, J. 2018. High-speed data in Africa: an assessment of provision via mobile networks. *Digital Policy, Regulation and Governance,* 20**,** 23-41.

DANIEL, E. M.-J., O.; & M., P. S. A. E. 2011. The Hummingbird-2 Lightweight

Authenticated Encryption Algorithm. *Springer***,** 19-31.

EL ZOUKA, H. A. An authentication scheme for wireless healthcare monitoring sensor network. 2017 14th International Conference on Smart Cities: Improving Quality of Life Using ICT and IoT, HONET-ICT 2017, 2017. 68-73.

FAN, K., WANG, W., WANG, Y., LI, H. & YANG, Y. Cloud-based lightweight RFID healthcare privacy protection protocol. 2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings, 2016.

FERRAG ET AL., L. M., ANTONIOS ARGYRIOU, DIMITRIOS KOSMANOS, AND HELGE JANICKE 2017. Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes. *Journal of Network and Computer Applications,* 101(2018)**,** 55-82.

FREUDENTHAL, V. H., IMBI NÕGISTO 2015. X-Road Architecture Technical Specification. *Cybernetica,* 1(1)**,** 1-15.

GAOBOTSE, G., MBUNGE, E., BATANI, J. & MUCHEMWA, B. 2022. The future of smart implants towards personalized and pervasive healthcare in Sub-Saharan Africa: Opportunities, barriers and policy recommendations. *Sensors International,* 3.

GURUMANAPALLI, K. P. & MUTHULURU, N. 2021. Feistel Network Assisted Dynamic Keying based SPN Lightweight Encryption for IoT Security. *International Journal of Advanced Computer Science and Applications,* 12**,** 377-392.

IMANE, S., TOMADER, M. & NABIL, H. Comparison between CoAP and MQTT in Smart Healthcare and Some Threats. International Symposium on Advanced Electrical and Communication Technologies, ISAECT 2018 - Proceedings, 2019.

JAGADEESWARI, V., SUBRAMANIYASWAMY, V., LOGESH, R. & VIJAYAKUMAR, V. 2018. A study on medical Internet of Things and Big Data in personalized healthcare system. *Health Information Science and Systems,* 6(1)**,** 14.

JAHAN, N., NAVEED, S., ZESHAN, M. & TAHIR, M. A. 2016. How to Conduct a Systematic Review: A Narrative Literature Review. *Cureus,* 8**,** e864.

KUMAR, P. & LEE, H. J. 2012. Security issues in healthcare applications using wireless medical sensor networks: a survey. *Sensors (Basel),* 12(1)**,** 55-91.

KUMAR, P., PORAMBAGE, P., YLIANTTILA, M., GURTOV, A., LEE, H. J. & SAIN, M. Addressing a secure session-key scheme for mobility supported e-Healthcare systems. International Conference on Advanced Communication Technology, ICACT, 2014. 538-540.

LATIF, S., QADIR, J., FAROOQ, S. & IMRAN, M. A. 2017. How 5G Wireless (and Concomitant Technologies) Will Revolutionize Healthcare? *Future Internet,* 9.

LIBERATI, A., ALTMAN, D. G., TETZLAFF, J., MULROW, C., GØTZSCHE, P. C., IOANNIDIS, J. P. A., CLARKE, M., DEVEREAUX, P. J., KLEIJNEN, J. & MOHER, D. 2009. The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. *PLoS Medicine,* 6(7)**,** 1000100.

LUNA, R., RHINE, E., MYHRA, M., SULLIVAN, R. & KRUSE, C. S. 2016. Cyber threats to health information systems: A systematic review. *Technology and Health Care,* 24(1)**,** 1-9.

MALILA, B. & MUTSVANGWA, T. E. M. 2019. Security architecture for a 5G mHealth system. *Global Health Innovation,* 2(1)**,** 1.

MEDILEH, S., LAOUID, A., NAGOUDI, E. M. B., EULER, R., BOUNCEUR, A., HAMMOUDEH, M., ALSHAIKH, M., ELEYAN, A. & KHASHAN, O. A. 2020. A flexible encryption technique for the internet of things environment. *Ad Hoc Networks,* 106.

MEMON, Q. A. & MUSTAFA, A. F. 2015. Exploring mobile health in a private online social network. *International Journal of Electronic Healthcare,* 8(1)**,** 51-75.

MEMON, R., LI, J. & AHMED, J. 2019. Simulation Model for Blockchain Systems Using Queuing Theory. *Electronics,* 8(2)**,** 234.

MOHER, D., LIBERATI, A., TETZLAFF, J., ALTMAN, D. G. & THE, P. G. 2009. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLOS Medicine,* 6**,** e1000097.

MWANGAMA, J., MALILA, B., DOUGLAS, T. & RANGAKA, M. 2020. What can 5G do for healthcare in Africa? *Nature Electronics,* 3(1)**,** 7-9.

PAHLEVAN-SHARIF, S., MURA, P. & WIJESINGHE, S. N. R. 2019. A systematic review of systematic reviews in tourism. *Journal of Hospitality and Tourism Management,* 39**,** 158-165.

PATI, D. & LORUSSO, L. N. 2018. How to Write a Systematic Review of the Literature. *Herd,* 11(1)**,** 15-30.

PEÑA, C. A. N., DÍAZ, A. E. G., AGUIRRE, J. A. A. & MOLINA, J. M. M. Security model to protect patient data in mHealth systems through a Blockchain network. Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology, 2019.

RAMLI, S. N., AHMAD, R., ABDOLLAH, M. F. & DUTKIEWICZ, E. A biometric-based security for data authentication in Wireless Body Area Network (WBAN). International Conference on Advanced Communication Technology, ICACT, 2013. 998-1001.

SAMAOUI, S., EL BOUABIDI, I., OBAIDAT, M. S., ZARAI, F. & MANSOURI, W. 2015. Wireless and mobile technologies and protocols and their performance evaluation. *Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications.*

SINGH, D., KUMAR, B., SINGH, S. & CHAND, S. 2021. A secure iot-based mutual authentication for healthcare applications in wireless sensor networks using eCC. *International Journal of Healthcare Information Systems and Informatics,* 16**,** 21-48.

SRIDHARAN, K. 2010. Security Vulnerabilities In Wireless Sensor Networks: A Survey. *Journal of Information Assurance and Security,* 5(1)**,** 31-44.

TAN, C. C., ZHONG, S., WANG, H. & LI, Q. Body sensor network security: An identity-based cryptography approach. WiSec'08: Proceedings of the 1st ACM Conference on Wireless Network Security, 2008. 148-153.

TAN, Z. 2018. Secure Delegation-Based Authentication for Telecare Medicine Information Systems. *IEEE Access,* 6**,** 26091-26110.

TIAN, S., YANG, W., GRANGE, J. M. L., WANG, P., HUANG, W. & YE, Z. 2019. Smart healthcare: making medical care more intelligent. *Global Health Journal,* 3(3)**,** 62-65.

VISWANATHAN, M., PATNODE, C. D., BERKMAN, N. D., BASS, E. B., CHANG, S., HARTLING, L., MURAD, M. H., TREADWELL, J. R. & KANE, R. L. 2017. Assessing the Risk of Bias in Systematic Reviews of Health Care Interventions. *Methods Guide for Effectiveness and Comparative Effectiveness Reviews.* The Scientific Resource Center.

ZGHAIBEH, M., FAROOQ, U., HASAN, N. U. & BAIG, I. 2020. SHealth: A Blockchain-Based Health System with Smart Contracts Capabilities. *IEEE Access,* 8(1)**,** 70030-70043.

8. Appendix

8.1. Appendix A

8.1.1. Search strategy from different databases

Table A1 Scopus Search Strategy

Number	Description	Query	Items Found
#1	Free Text	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain	1,160,840
#2	Free Text	4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*”	254,552
#3	#1 AND #2	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*”	39,222
#4	Free Text	Health	4,896,914
#5	#3 AND #4	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*” AND Health	1,819
#6	Add Filter	DOCTYPE , "ar" OR "cp" OR "ch"	1,494
#7	Add Filter	LANGUAGE , "English"	1,475
#8	Add Filter	Abstract, Author keywords, Index keywords	**795**

Table A2 PubMed Search Strategy

Number	Description	Query	Items Found
#1	Free Text	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain	213,982
#2	Mesh terms	"Blockchain"[Mesh]	96
#3	Free Text	4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*”	11,439
#4	#1 OR #2 AND #3	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain OR "Blockchain"[Mesh] 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*”	143
#5	Free Text	Health	2,033,083
#6	#4 AND #5	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain OR "Blockchain"[Mesh] 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*” AND Health	27

#7	Add Filter	DOCTYPE , "ar" OR "cp" OR "ch"	0
#8	Add Filter	LANGUAGE , "English"	0

Table A3 Web of Science Search Strategy

Number	Description	Query	Items Found
#1	Free Text	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain	500,705
#2	Free Text	4G OR 5G OR "Fourth-generation" OR "Fifth-generation" OR "Mobile network*"	38,155
#3	#1 AND #2	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR "Fourth-generation" OR "Fifth-generation" OR "Mobile network"	2,011
#4	Free Text	Health	2,305,290
#5	#3 AND #4	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR "Fourth-generation" OR "Fifth-generation" OR "Mobile network" AND Health	1,067
#6	Add Filter	DOCTYPE , "ar" OR "cp" OR "ch"	533
#7	Add Filter	LANGUAGE , "English"	**483**

Table A4 Medline via Web of Science Search Strategy

Number	Description	Query	Items Found
#1	Free Text	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain	242,124
#2	Free Text	4G OR 5G OR "Fourth-generation" OR "Fifth-generation" OR "Mobile network*"	18,356
#3	#1 AND #2	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR "Fourth-generation" OR "Fifth-generation" OR "Mobile network*"	219
#4	Free Text	Health	3,027,249
#5	#3 AND #4	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR "Fourth-generation" OR "Fifth-generation" OR "Mobile network" AND Health	40
#6	Add Filter	DOCTYPE , "ar" OR "cp" OR "ch"	29
#7	Add Filter	LANGUAGE , "English"	**28**

Table A5 CINAL via EBSCO host Search Strategy

Number	Description	Query	Items Found
#1	Free Text	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain	91 397
#2	Free Text	4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network”	881
#3	#1 AND #2	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network*”	92 052
#4	Free Text	Health	1 802 194
#5	#3 AND #4	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network” AND Health	92 034
#6	Add Filter	DOCTYPE , "ar" OR "cp" OR "ch"	0
#7	Add Filter	LANGUAGE , "English"	**0**

Table A6 Cochrane Library via Web of Science Search Strategy

Number	Description	Query	Items Found
#1	Free Text	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain	51 036
#2	Free Text	4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network”	2 252
#3	#1 AND #2	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network”	2 751
#4	Free Text	Health	7 779
#5	#3 AND #4	Security OR Privacy OR Confidentiality OR Integrity OR Authentication OR Blockchain AND 4G OR 5G OR “Fourth-generation” OR “Fifth-generation” OR “Mobile network” AND Health	2 751
#6	Add Filter	DOCTYPE , "ar" OR "cp" OR "ch"	0
#7	Add Filter	LANGUAGE , "English"	**0**

8.2. Appendix B

8.2.2. Data Extraction Forms

8.2.2.1. Data Extraction Form sample

Form B1 Security for Smart Healthcare Systems

Form completed by:
Author (year):
Full reference:
Problem:
Is study eligible for inclusion (yes/no):
If not eligible, provide reasons:
Intervention(s) / Security measures proposed:
Outcomes:
Findings/Results:
Authors' Conclusions:
Authors' description of security requirements for smart health:
Effectiveness of proposed security measures:
Type of Study:
Country of Study:
Type of Intervention:
Type of security issue:
Type of smart device:
Type of storage:
Type of outcome:

Comments:

8.2.2.2. Data Extraction Form for Included study
Form B2 Security for Smart Healthcare Systems

Form completed by: Perfect
Author (year): Afzal, I., S. A. Parah, N. N. Hurrah and O. Y. Song (2020)
Full reference: Afzal, I., S. A. Parah, N. N. Hurrah and O. Y. Song (2020). "Secure patient data transmission on resource constrained platform." Multimedia Tools and Applications. DOI: 10.1007/s11042-020-09139-3
Problem: The inability of resource constrained devices to provide health data security when being transmitted to a third party due to their limited processing capabilities and limited battery life.
Is study eligible for inclusion (yes/no): YES
If not eligible, provide reasons: N/A
Intervention(s) / Security measures proposed: A secure data transmission method using a complex encryption transmitting healthcare related data over the network by devices with resource constraint, as well as prevention of EHR modification by a third party. Two level encryption techniques were proposed to ensure high level of medical data security: Strong encryption (chaotic) to ensure that the cloud administrator is not able to modify the information such as an image sent to the cloud, and bitplane encryption which is done by the user on the entire set of data. It also provide a small encryption time which allows the security of health data on the cloud.
Outcomes: Development of a new framework for secure health data transmission using the encryption algorithm applied on the data before transmission.
Findings/Results: Authors have found that when doing the When doing the encryption of health data (An image for example) the image is divided into 4, allowing the client, the cloud administrator and the user to encrypt part of the image simultaneously. When doing the Strong encryption (chaotic) the third party does the encryption then the light weight encryption is done by client.
Authors' Conclusions: Authors concluded that the issue of transmitting data through insecure networks of resource constraints platforms has been resolved by entrusting the splitting of encryption of data with the third-party but at the same time ensuring the privacy and security of transmitted data as well as the reduction in encryption time.
Authors' description of security requirements for smart health: Client needs to be connected to the cloud and the cloud has to be trustworthy

Effectiveness of proposed security measures: A two-level encryption has provided security for medical data over cloud and reduced encryption time.
Type of Study: Qualitative
Country of Study: South Korea
Type of Intervention: Encryption based data transmission method
Type of security issue: Network security (Data transmission)
Type of smart device: Medical devices or smart phones
Type of storage: Cloud storage
Type of outcome: Security of electronic health record
Comments: None

8.2.2.3. Data Extraction Form for Excluded study

Form B3 Security for Smart Healthcare Systems

Form completed by: Perfect
Author (year): Boussada, R., B. Hamdaney, M. E. Elhdhili, S. Argoubi and L. A. Saidane (2018)
Full reference: Boussada, R., B. Hamdaney, M. E. Elhdhili, S. Argoubi and L. A. Saidane (2018). A Secure and Privacy-Preserving Solution for IoT over NDN Applied to E-health. 2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018. DOI: 10.1109/IWCMC.2018.8450374
Problem: Privacy and security challenges in IoT
Is study eligible for inclusion (yes/no): NO
If not eligible, provide reasons: This study focuses on the security analysis of an existing security solution. This paper is excluded because it is not focusing on medical data protection at the acquisition device, security of data while being transferred through mobile networks, or the security of data at the storage device.
Intervention(s) / Security measures proposed: N/A
Outcomes: N/A
Findings/Results: N/A
Authors' Conclusions: N/A
Authors' description of security requirements for smart health: N/A
Effectiveness of proposed security measures: N/A
Type of Study: N/A
Country of Study: N/A
Type of Intervention: N/A
Type of security issue: N/A
Type of smart device: N/A
Type of storage: N/A
Type of outcome: N/A
Comments: N/A

8.3. Appendix C

8.3.1. Exclusion and Inclusion criteria table

Characteristic	Inclusion criteria	Exclusion criteria
Problem	Articles on security in smart healthcare systems for patient data sharing, storage and access control. Patient data	Articles that do not focus on health related topics are excluded. Patient data
Intervention	Studies focusing on the security mechanisms used to mitigate against data breaches in smart healthcare systems. risks measures in smart healthcare systems	Articles that do not demonstrate data protection at the acquisition device, security of data while being transferred through mobile networks, or the security of data at the storage device are excluded.
Outcome	Studies on improved security of smart healthcare systems for patient data sharing, storage and access control. Smart healthcare systems for patient data in terms of security, sharing, storage and access control.	

8.4. Appendix D

8.4.1. A comprehensive table of reasons for exclusion from the 164 studies checked for eligibility

Author	Title	Reason for exclusion
Aliasgari, M., M. Black and N. Yadav (2019).	Security vulnerabilities in mobile health applications.	Excluded on basis of publication type: Analysis paper
Al-Sharo, Y. M. (2019).	Networking issues for security and privacy in mobile health apps	Excluded on basis of publication type: Analysis paper
Atat, R., L. Liu, J. Wu, G. Li, C. Ye and Y. Yang (2018).	Big Data Meet Cyber-Physical Systems: A Panoramic Survey.	Excluded on basis of publication type: Survey paper
Belkhouja, T., A. Mohamed, A. K. Al-Ali, X. Du and M. Guizani (2017).	Light-weight encryption of wireless communication for implantable medical devices using henon chaotic system.	Excluded on basis of publication type: Analysis paper
Benssalah, M., M. Djeddou and K. Drouiche (2016).	"Dual cooperative RFID-telecare medicine information system authentication protocol for healthcare environments."	Excluded on basis of publication type: Review paper
Binu, P. K., K. Thomas and N. P. Varghese (2017).	Highly secure and efficient architectural model for IoT based health care systems.	Excluded on the basis of not relating to medical data protection
Boussada, R., B. Hamdaney, M. E. Elhdhili, S. Argoubi and L. A. Saidane (2018).	A Secure and Privacy-Preserving Solution for IoT over NDN Applied to E-health.	Excluded on basis of publication type: Analysis paper
Braeken, A. and M. Liyanage (2020).	"Highly efficient key agreement for remote patient monitoring in MEC-enabled 5G networks."	Excluded on the basis of study focus: not relating to medical data protection
Chaudhry, J., K. Saleem, R. Islam, A. Selamat, M. Ahmad and C. Valli (2017).	AZSPM: Autonomic Zero-Knowledge Security Provisioning Model for Medical Control Systems in Fog Computing Environments.	Excluded on the basis of study focus: Hardware component of medical devices
Chen, B., S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu and Y. Zhai (2020).	"A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture."	Excluded on the basis of study focus: Focuses on proving security awareness of 5G based smart medical platform

Chen, C. M., B. Xiang, T. Y. Wu and K. H. Wang (2018).	"An anonymous mutual authenticated key agreement scheme for wearable sensors in Wireless Body Area Networks."	Excluded on basis of publication type: analysis study
Chen, W., Z. Chen and F. Cui (2019).	"Collaborative and secure transmission of medical data applied to mobile healthcare."	Excluded on the basis of study focus: Policy in healthcare system
Chen, Z., F. Zhang, P. Zhang, J. K. Liu, J. Huang, H. Zhao and J. Shen (2018).	"Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control."	Excluded on the basis of study focus: Search of data in healthcare system
Chowdhury, M. Z., M. T. Hossan, M. Shahjalal, M. K. Hasan and Y. M. Jang (2020).	"A New 5G eHealth Architecture Based on Optical Camera Communication: An Overview, Prospects, and Applications."	Excluded on the basis of study focus: Connectivity provision
Chung, K. and H. Jung (2019).	"Knowledge-based block chain networks for health log data management mobile service."	Excluded on the basis of study focus: Data capturing
Clim, A., R. D. Zota and R. Constantinescu (2019).	Data exchanges based on blockchain in m-health applications.	Excluded on basis of publication type: Analysis paper
Das, A. K. (2015).	"A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems."	Excluded on basis of publication type: Analysis paper
Das, A. K., V. Odelu and A. Goswami (2015).	"A Secure and Robust User Authenticated Key Agreement Scheme for Hierarchical Multi-medical Server Environment in TMIS."	Excluded on basis of publication type: Analysis paper
Deng, J., C. Xu, H. Wu and J. Chen (2016).	"Analysis and improvement of a fair remote retrieval protocol for private medical records."	Excluded on basis of publication type :Analysis paper
Ding, D., M. Conti and A. Solanas (2016).	A smart health application and its related privacy issues.	Excluded on basis of publication type: Analysis paper
Eldeib, A. M. (2014).	"Interactive telemedicine solution based on a secure mHealth application."	Excluded on the basis of study focus: Affordability of Electronic Health record (EHR)

Elhai, J. D. and B. C. Frueh (2016).	"Security of electronic mental health communication and record-keeping in the digital age."	Excluded on the basis of study focus: Designing a Software for system security
Els, F. and L. Cilliers (2017).	Improving the information security of personal electronic health records to protect a patient's health information.	Excluded on basis of publication type: Analysis paper
Fatima, R., R. Manal and M. Tomader (2019).	Cryptography in e-Health using 5G based IOT: A comparison study.	Excluded on basis of publication type: Analysis and comparison paper
Feng, B., V. Thuan Do, N. Jacot, B. Santos, B. Dzogovic, E. Brandsma and T. van Do (2019).	Secure 5G Network Slicing for Elderly Care.	Excluded on the basis of study focus: Implementation of 5G in home based care does not focus on security of EHR
Gochhayat, S. P., C. Lal, L. Sharma, D. P. Sharma, D. Gupta, J. A. M. Saucedo and U. Kose (2020).	"Reliable and secure data transfer in IoT networks."	Excluded on the basis of study focus: Management to the IoT ecosystem
Gottschlich, S. (2017).	Incorporating health monitoring and duress detection into mobile device authentication.	Excluded on the basis of study focus: Security of mobile device
Guillen-Gamez, F. D., I. Garcia-Magarino, J. Bravo-Agapito, R. Lacuesta and J. Lloret (2017).	"A proposal to improve the authentication process in m-health environments."	Excluded on the basis of study focus: Facial authentication through database comparison
Hasan, R., S. Zawoad, S. Noor, M. M. Haque and D. Burke (2016).	How Secure is the Healthcare Network from Insider Attacks?	Excluded on basis of publication type: Systematic review paper
Haraty, R. A., M. Zbib and M. Masud (2016).	"Data damage assessment and recovery algorithm from malicious attacks in healthcare data sharing systems."	Excluded on the basis of study focus: recovering deleted data
Hawig, D., C. Zhou, S. Fuhrhop, A. S. Fialho and N. Ramachandran (2019).	"Designing a distributed ledger technology system for interoperable and general data protection regulation–compliant health data exchange: A use case in blood glucose data."	Excluded on the basis of study focus: Design of a data exchange system

Huertas Celdrán, A., M. Gil Pérez, F. J. García Clemente and G. Martínez Pérez (2018).	"Sustainable securing of Medical Cyber-Physical Systems for the healthcare of the future."	Excluded on the basis of study focus: Design of a policy system for health data
Humayun, M., N. Z. Jhanjhi, M. Alruwaili, S. S. Amalathas, V. Balasubramanian and B. Selvaraj (2020).	"Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things."	Excluded on the basis of study focus: Description of 5G technology
Hussain, S. Z. and M. Kumar (2019).	Secret Key Agreement Schemes in IOT Based Wireless Body Area Network.	Excluded on basis of publication type: Analysis paper
Ichikawa, D., M. Kashiyama and T. Ueno (2017).	"Tamper-resistant mobile health using blockchain technology."	Excluded on basis of publication type: Analysis paper
Izaara, A. A., R. Ssembatya and F. Kaggwa (2019).	An access control framework for protecting personal electronic health records.	Excluded on basis of publication type: Review paper
Jang, K. and O. Lee (2020).	"The design and development of a blockchain based epro system for collecting clinical data."	Excluded on the basis of study focus: Design of a blockchain system
Jiang, Q., X. Lian, C. Yang, J. Ma, Y. Tian and Y. Yang (2016).	"A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth."	Excluded on basis of publication type: Analysis paper
Jiang, S., X. Zhu and L. Wang (2015).	"EPPS: Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks."	Excluded on the basis of study focus: Policy of health data
Jiang, S., X. Zhu, R. Hao, H. Chi, H. Li and L. Wang (2015).	Lightweight and privacy-preserving agent data transmission for mobile Healthcare.	Excluded on the basis of study focus: Unavailability of patient device
Jusak, J., H. Pratikno and V. H. Putra (2017).	Internet of Medical Things for cardiac monitoring: Paving the way to 5G mobile networks.	Excluded on the basis of study focus: Prototype for IoMT
Kalake, L. and C. Yoshida (2018).	Designing an Electronic Health Security System Framework for Authentication with Wi-Fi, Smartphone and 3D Face Recognition Technology.	Excluded on the basis of study focus: Security of mobile device

Kamarudin, N. H. and Y. M. Yussoff (2016).	Authentication scheme interface for mobile e-health monitoring using unique and lightweight identity-based authentication.	Excluded on basis of publication type: Analysis paper
Kao, J. H., W. C. Wu, L. M. Hsu and H. T. Liaw (2020).	A Research on Real-Name Blockchain System Bind Health Passbook Electronic Medical Record Exchanges Mechanism.	Excluded on the basis of study focus: Design of a passbook and smart cards
Karamachoski, J. and L. Gavrilovska (2019).	Framework for next generation of digital healthcare systems.	Excluded on the basis of study focus: evolution of eHealth systems
Kavitha, D. and C. Subramaniam (2017).	"Security threat management by software obfuscation for privacy in internet of medical thing (IoMT) application."	Excluded on the basis of study focus: Software management
Kaw, J. A., N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh and G. M. Bhat (2019).	"A reversible and secure patient information hiding system for IoT driven e-health."	Excluded on the basis of study focus: protection of cloud administration in cloud-based platforms.
Kim, J. T. (2017).	"On the attack model and vulnerability for mobile healthcare system."	Excluded on basis of publication type: Analysis paper
Kong, F., Y. Zhou, B. Xia, L. Pan and L. Zhu (2019).	"A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment."	Excluded on basis of publication type: Analysis paper
Kumar, S., B. Mahapatra, R. Kumar and A. K. Turuk (2018).	Security and privacy solution for I-RFID based smart infrastructure health monitoring.	Excluded on the basis of study focus: delivery of healthcare through smart cities
Li, C. T., D. H. Shih and C. C. Wang (2018).	"Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems."	Excluded on basis of publication type: Analysis paper
Li, X., J. Niu, S. Kumari, J. Liao, W. Liang and M. K. Khan (2016).	"A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity."	Excluded on basis of publication type: Analysis paper

Li, X., J. Peng, M. S. Obaidat, F. Wu, M. K. Khan and C. Chen (2020).	"A Secure Three-Factor User Authentication Protocol with Forward Secrecy for Wireless Medical Sensor Network Systems."	Excluded on basis of publication type: Analysis paper
Liang, X., S. Shetty, D. Tosh, D. Bowden, L. Njilla and C. Kamhoua (2018).	"Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications."	Excluded on the basis of study focus: development of web based personal health system
Lim, H. A., P. D. T. Vy and J. Choi (2019).	"Detecting knowledge structures in artificial intelligence and medical healthcare with text mining."	Excluded on basis of publication type: Analysis paper
Liu, W., J. Liu, Q. Wu, W. Susilo, H. Deng and B. Qin (2016).	"SAKE: scalable authenticated key exchange for mobile e-health networks."	Excluded on the basis of study focus: network security architecture
Lloret, J., S. Sendra, J. M. Jimenez and L. Parra (2016).	"Providing security and fault tolerance in P2P connections between clouds for mHealth services."	Excluded on the basis of study focus: provision of security and storage resources
Lotfy, K. and M. L. Hale (2016).	Assessing pairing and data exchange mechanism security in the wearable internet of things.	Excluded on the basis of study focus: Connection of wearable medical devices
Lu, Y., L. Li, H. Peng, D. Xie and Y. Yang (2015).	"Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps."	Excluded on basis of publication type: Analysis paper
Mamta and B. Gupta (2020).	"An attribute-based keyword search for m-Health networks."	Excluded on the basis of study focus: search done over encrypted data in m-health network
Marin, E., M. A. Mustafa, D. Singelée and B. Preneel (2016).	A privacy-preserving remote healthcare system offering end-to-end security.	Excluded on the basis of study focus: design of healthcare system
Mehmood, Z., A. Ghani, G. Chen and A. S. Alghamdi (2019).	"Authentication and secure key management in e-health services: A robust and efficient protocol using biometrics."	Excluded on basis of publication type: Analysis paper
Mense, A., S. Steger, M. Sulek, D. Jukicsunaric and A. Mészáros (2016).	Analyzing privacy risks of mhealth applications	Excluded on basis of publication type: Analysis paper

Mishra, K. N. (2020).	An efficient approach towards enhancing the performance of m-health using sensor networks and cloud technologies.	Excluded on the basis of study focus: the description of a remote health management system
Mishra, K. N. (2020).	Supervising data transmission services using secure cloud based validation and admittance control mechanism.	Excluded on the basis of study focus: metamorphosis utility of mobile health data transmission
Mohanta, B., P. Das and S. Patnaik (2019).	Healthcare 5.0: A paradigm shift in digital healthcare system using artificial intelligence, IOT and 5G communication.	Excluded on basis of publication type: Summary and Analysis paper
Moosavi, S. R., T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen and J. Isoaho (2015).	Session resumption-based end-to-end security for healthcare internet-of-things.	Excluded on the basis of study focus: development of a prototype for patient monitoring based on IoT system
Moss, L., M. Shaw, I. Piper, C. Hawthorne and J. Kinsella (2017).	Sharing of big data in healthcare: Public opinion, trust, and privacy considerations for health informatics researchers.	Excluded on basis of publication type: Analysis paper
Motohashi, T., T. Hirano, K. Okumura, M. Kashiyama, D. Ichikawa and T. Ueno (2019).	"Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation."	Excluded on the basis of study focus: design and validation of a mhealth system
Mustafa, U. and N. Philip (2019).	Group-Based Key Exchange for Medical IoT Device-to-Device Communication (D2D) Combining Secret Sharing and Physical Layer Key Exchange.	Excluded on the basis of study focus: design of a key management
Nasri, F. and A. Mtibaa (2017).	"Smart Mobile Healthcare System based on WBSN and 5G."	Excluded on the basis of study focus: design of a general architecture IoT based
Nwebonyi, F. N., R. Martins and M. E. Correia (2019).	Security and Fairness in IoT Based e-Health System: A Case Study of Mobile Edge-Clouds.	Excluded on the basis of study focus: description of IoT based e-health
Park, H. A. and C. Su (2019).	"Secure Information Sharing System for Online Patient Networks."	Excluded on basis of publication type: Analysis paper

Park, Y. R., E. Lee, W. Na, S. Park, Y. Lee and J. H. Lee (2019).	"Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility."	Excluded on basis of publication type: Investigative paper
Periyasamy, K. and S. Alsyefi (2019).	Implementation of security and privacy aspects in a healthcare social network.	Excluded on the basis of study focus: Design of a healthcare network
Piliouras, T. C., R. J. Suss, P. L. Yu, S. V. Kachalia, R. S. Bangera, R. R. Kalra and M. P. Maniyar (2015).	The rise of mobile technology in healthcare: The challenge of securing teleradiology.	Excluded on the basis of study focus: Security of mobile device
Plamondon, R., G. Pirlo, É. Anquetil, C. Rémi, H. L. Teulings and M. Nakagawa (2018).	"Personal digital bodyguards for e-security, e-learning and e-health: A prospective survey."	Excluded on basis of publication type: Survey paper
Preetha, A. D. and T. S. P. Kumar (2019).	MLPPT-MHS: Multi-Layered Privacy Preserving and Traceable Mobile Health System.	Excluded on basis of publication type: Investigative paper
Qiu, H., M. Qiu, M. Liu and G. Memmi (2020).	"Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0."	Excluded on the basis of study focus: design of system architecture
Rath, M. and B. Pattanayak (2019).	"Technological improvement in modern health care applications using Internet of Things (IoT) and proposal of novel health care approach."	Excluded on basis of publication type: Analysis paper
Rathore, H., A. Al-Ali, A. Mohamed, X. Du and M. Guizani (2018).	DTW based Authentication for Wireless Medical Device Security.	Excluded on the basis of study focus: Security of medical device
Reinsmidt, E., D. Schwab and L. Yang (2016).	Securing a Connected Mobile System for Healthcare.	Excluded on basis of publication type: Analysis paper
Renardi, M. B., N. C. Basjaruddin and E. Rakhman (2018).	"Securing electronic medical record in Near Field Communication using Advanced Encryption Standard (AES)."	Excluded on basis of publication type: Analysis paper

Saha, H. N., D. Paul, S. Chaudhury, S. Haldar and R. Mukherjee (2017).	Internet of Thing based healthcare monitoring system.	Excluded on basis of publication type: Review paper
Santhi Vandana, T., S. Venkateshwarlu and C. V. Ravi Teja (2019).	"Exploration of an intelligent and secure wireless body area networks for health monitoring."	Excluded on basis of publication type: Survey paper
Seepers, R. M., C. Strydis, I. Sourdis and C. I. De Zeeuw (2017).	"Enhancing Heart-Beat-Based Security for mHealth Applications."	Excluded on basis of publication type: Analysis paper
Selvakanmani, S., M. Shanmathi and N. S. Sandhya (2019).	Cluster-based health monitoring scheme in wireless sensor networks.	Excluded on the basis of study focus: design of a wireless sensor network
Sengupta, S. (2020).	A Secured Biometric-Based Authentication Scheme in IoT-Based Patient Monitoring System.	Excluded on basis of publication type: Analysis paper
Sethia, D., D. Gupta, H. Saran, R. Agrawal and A. Gaur (2016).	Mutual authentication protocol for secure NFC based mobile healthcard.	Excluded on the basis of study focus: design of architecture for smart heath cards
Sethuraman, S. C., V. Vijayakumar and S. Walczak (2020).	"Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles."	Excluded on the basis of study focus: development of aerial vehicles
Shah, A., H. Abbas, W. Iqbal and R. Latif (2018).	Enhancing E-Healthcare Privacy Preservation Framework through L-Diversity.	Excluded on basis of publication type: Analysis paper
Shahbodin, F., A. H. Azni, T. Ali and C. K. N. C. K. Mohd (2019).	Lightweight cryptography techniques for MHealth cyber security.	Excluded on basis of publication type: Survey paper
Sharma, B., C. N. Sekharan and F. Zuo (2018).	Merkle-Tree Based Approach for Ensuring Integrity of Electronic Medical Records.	Excluded on the basis of study focus: Innovation to healthcare system
Sindhuja, L. S. (2019).	Security of healthcare monitoring system using EHIP-HOP method.	Excluded on the basis of study focus: healthcare system monitoring
Singh, D., B. Kumar, S. Singh and S. Chand (2021).	"A secure iot-based mutual authentication for healthcare applications in wireless sensor networks using eCC."	Excluded on basis of publication type: Analysis paper

Sowmiya, E., L. Malathi and A. Thamarai Selvi (2016).	"A study on security issues in healthcare applications using medical wireless sensor network and IoT."	Excluded on basis of publication type: Analysis paper
Suhardi and A. Ramadhan (2016).	A survey of security aspects for internet of things in healthcare	Excluded on basis of publication type: Survey paper
Sun, Y. (2016).	"An improved password authentication scheme for telecare medical information systems based on chaotic maps with privacy protection."	Excluded on basis of publication type: Analysis paper
Sureshkumar, V., R. Amin, V. R. Vijaykumar and S. R. Sekar (2019).	"Robust secure communication protocol for smart healthcare system with FPGA implementation."	Excluded on basis of publication type: Analysis paper
Tan, Z. (2014).	"A user anonymity preserving three-factor authentication scheme for telecare medicine information systems."	Excluded on basis of publication type: Analysis paper
Tan, Z. (2018).	"Secure Delegation-Based Authentication for Telecare Medicine Information Systems."	Excluded on basis of publication type: Analysis paper
Tawalbeh, L. A., H. Tawalbeh, H. Song and Y. Jararweh (2017).	Intrusion and attacks over mobile networks and cloud health systems.	Excluded on the basis of study focus: technologies associated with mobile and cloud-base smart
Tawalbeh, L. A., W. Bakhader, R. Mehmood and H. Song (2016).	Cloudlet-based mobile cloud computing for healthcare applications.	Excluded on the basis of study focus: mobile device connection
Tembhare, A., S. Sibi Chakkaravarthy, D. Sangeetha, V. Vaidehi and M. Venkata Rathnam (2019).	"Role-based policy to maintain privacy of patient health records in cloud."	Excluded on the basis of study focus: role assignment and permissions within the healthcare system
Thamilarasu, G. and C. Lakin (2017).	A security framework for mobile health applications.	Excluded on the basis of study focus: lack of awareness on security issues for mobile applications

Thayananthan, V. (2019).	"Healthcare Management using ICT and IoT based 5G."	Excluded on basis of publication type: Investigative paper
Abiramy, N. V. and S. V. Sudha (2019)	A secure and lightweight authentication protocol for multiple layers in wireless body area network	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Acharya, S., B. Ehrenreich and J. Marciniak (2015)	OWASP inspired mobile security	Excluded on the basis of study focus: Methodology development
Ahmed, S. (2019)	BYOD, personal area networks (PANs) and IOT: Threats to patient's privacy	Excluded on basis of publication type: Survey paper
Alshamsi, A. Z., E. S. Barka and M. A. Serhani (2017)	Lightweight encryption algorithm in wireless body area network for e-health monitoring	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Alshehri, M. (2019)	A novel Secure wireless healthcare applications for medical community	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Alzahrani, B. A. (2020)	Secure and Efficient Cloud-based IoT Authenticated Key Agreement scheme for e-Health Wireless Sensor Networks	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Amin, R., S. H. Islam, G. P. Biswas, M. K. Khan and N. Kumar (2018)	A robust and anonymous patient monitoring system using wireless medical sensor networks	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Amin, M., D. Shehwar, A. Ullah, T. Guarda, T. A. Tanveer and S. Anwar (2020).	A deep learning system for health care IoT and smartphone malware detection	Excluded on the basis of study focus: lack of end to end security as this study focuses only Security threats

Ara, A., Jr., M. Al-Rodhaan, Y. Tian and A. Al-Dhelaan (2017).	A Secure Privacy-Preserving Data Aggregation Scheme Based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Atri, K., Y. M. Bangera, V. S. Deshmukh and V. Vijayakumar (2019).	Privacy Preservation and Signature Aggregation for Medical Data	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Azeez, N. A. and C. V. D. Vyver (2018).	Dynamic Patient-Regulated Access Control Framework for Electronic Health Information	Excluded on the basis of study focus: lack of end to end security as this study focuses only on data accessibility
Buddesab, J. Thriveni, M. S. Yashaswini and K. R. Venugopal (2018)	Efficient Secure and Private Healthcare Data Transmission and Allocation in Cloud Environment	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Buddesab, J. Thriveni, M. S. Yashaswini and K. R. Venugopal (2018)	Efficient Secure and Private Healthcare Data Transmission and Allocation in Cloud Environment	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Butt, S. A., J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco and M. Shoaib (2019)	IoT Smart Health Security Threats	Excluded on the basis of study focus: lack of end to end security as this study focuses only Security threats
Coppolino, L., S. D'Antonio, L. Romano, L. Sgaglione, M. Magliulo and R. Pacelli (2019)	Protecting critical business processes of smart hospitals from cyber-attacks	Excluded on the basis of study focus: lack of end to end security as this study focuses only Cyber security issues
El Ghoubach, I., F. Mrabti and R. Ben Abbou (2016)	Efficient secure and privacy preserving data access control scheme for multi-Authority personal health record systems in cloud computing	Excluded on the basis of study focus: lack of end to end security as this study focuses only on data accessibility

El Zouka, H. A. (2017).	An authentication scheme for wireless healthcare monitoring sensor network	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Fan, K., W. Wang, Y. Wang, H. Li and Y. Yang (2016)	Cloud-based lightweight RFID healthcare privacy protection protocol	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Ferebee, D., V. Shandilya, C. Wu, J. Ricks, D. Agular, K. Cole, B. Ray, A. Franklin, C. Titon and Z. Wang (2017)	A secure framework for mHealth data analytics with visualization	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Guan, Z., T. Yang, X. Du and M. Guizani (2016).	Secure data access for wireless body sensor networks	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Hathaliya, J. J., S. Tanwar and R. Evans (2020).	Securing electronic healthcare records: A mobile-based biometric authentication approach	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Hussien, Z. A., H. Jin, Z. A. Abduljabbar, M. A. Hussain, A. A. Yassin, S. H. Abbdal, M. A. Al Sibahee and D. Zou (2016)	Secure and efficient e-health scheme based on the Internet of Things	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Kalpally, A. T. and K. P. Vijayakumar (2021).	Privacy and security framework for health care systems in IoT: originating at architecture through application	Excluded on the basis of study focus: lack of end to end security as this study focuses only on data accessibility
Kamarudin, N. H., Y. M. Yussoff and H. Hashim (2015).	IBE-TRUST authentication for e-Health mobile monitoring system	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication

Khatoon, S., S. M. M. Rahman, M. Alrubaian and A. Alamri (2019).	Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Lee, Y. S., B. Ndibanje, E. Alasaarela, T. Kim and H. Lee (2015)	An effective and secure user authentication and key agreement scheme in m-healthcare systems	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Lei, C. L. and Y. H. Chuang (2019)	Privacy protection for telecare medicine information systems with multiple servers using a biometric-based authenticated key agreement scheme	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Li, X., M. H. Ibrahim, S. Kumari and R. Kumar (2018).	Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Li, C. T., C. C. Lee and C. Y. Weng (2016).	A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical Care System	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Liu, X., Y. Xia, W. Yang and F. Yang (2018).	Secure and efficient querying over personal health records in cloud computing	Excluded on the basis of study focus: lack of end to end security as this study focuses only on data accessibility
Lopes, A. P. G. and P. R. L. Gondim (2020)	Mutual authentication protocol for D2D communications in a cloud-based E-health system	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Lounis, A., A. Hadjidj, A. Bouabdallah and Y. Challal (2016)	Healing on the cloud: Secure cloud architecture for medical wireless sensor networks	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks

Parvez, M. K., F. T. Zohra and M. Jahan (2019)	A secure and lightweight user authentication mechanism for wireless body area network	Excluded on the basis of study focus: lack of end to end security as this study focuses on Wireless Body Area Networks
Pramila, R. S. and A. S. Nargunam (2016).	Enhancing security in real time patient monitoring	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Rahman, S. M. M., M. M. Masud, M. A. Hossain, A. Alelaiwi, M. M. Hassan and A. Alamri (2016).	Privacy preserving secure data exchange in mobile P2P cloud healthcare environment	Excluded on the basis of study focus: lack of end to end security as this study focuses only on data sharing
Sahoo, S. S. and S. Mohanty (2018).	Cloud-Assisted Privacy Preserving Authentication Scheme for Telecare Medical Information Systems	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication
Sammoud, A., M. A. Chalouf, O. Hamdi, N. Montavont and A. Bouallegue (2020)	A secure three-factor authentication and biometrics-based key agreement scheme for TMIS with user anonymity	Excluded on the basis of study focus: lack of end to end security as this study focuses only on data accessibility
Shamshad, S., Minahil, K. Mahmood, S. Kumari and C. M. Chen (2020).	A secure blockchain-based e-health records storage and sharing scheme	Excluded on the basis of study focus: lack of end to end security as this study focuses only on data accessibility
Silva, B. M. C., J. J. P. C. Rodrigues, F. Canelo, I. M. C. Lopes and J. Lloret (2019)	Towards a cooperative security system for mobile-health applications	Excluded on the basis of study focus: lack of end to end security as this study focuses only on authentication

8.5. Appendix E

8.5.1. Satnac Conference Peer Reviewed Paper

Security for networked smart healthcare systems: A systematic review

Nyamwezi Parfaite Ndarhwa[1], Bessie Malila[2]

[1,2]*Division of Biomedical Engineering, University of Cape Town, 7th Floor Anatomy Building, Observatory, Cape Town*

[1]ndrnya002@myuct.ac.za
[2]bessie.malila@uct.ac.za

Abstract— **Smart healthcare systems are connected to the Internet and use mobile platforms which allow them to utilize technologies such as wearable devices and Internet of Things (IoT) to dynamically connect people to health services and provide access to information related to healthcare. To secure and protect the sensitive medical information, several mitigation measures have been implemented and others have been proposed. Examples include data encryption and biometrics. Emerging security technologies such as Blockchain and X-Road, are expected to address the distributed and decentralized architectures of smart healthcare systems. This study reviewed studies that have addressed end-to-end security risks in smart healthcare systems. Most studies focused on the protection of patient's data from attackers who may cause harm. However, there is lack of studies that focus on protection data in cases where the intruder has already accessed the system.**

Keywords—**5G, security, smart healthcare, Blockchain, X-Road.**

I. Introduction

Smart healthcare systems are interconnected infrastructures comprising medical devices, health systems, and embedded technologies that are used for monitoring patients and deliver healthcare services [1]. Smart healthcare systems are set to transform healthcare, for example, through the use of applications installed on mobile devices which can be equipped with sensors for collecting physiological signals and health data. Smart healthcare services include teleconsultation, delivery of health information to practitioners, patients and healthcare service providers such as pharmacies, insurers, and researchers; remote real-time monitoring of vital signs; and training and collaboration of healthcare workers [2-4].

Mobile networks constitute one of the cornerstones of smart healthcare systems. Smart healthcare applications are installed on devices that use mobile networks. Mobile networks have experienced exponential growth over the years, the current fifth-generation networks (5G), will further drive the increased adoption of smart healthcare systems [5].

Certain security measures should be implemented to mitigate the security risks associated with connected health systems [6]. Security requirements for connected smart healthcare systems can be broken down into three key components, i.e. confidentiality, integrity, and availability. Confidentiality refers to the protection of data from being exposed to unauthorized users; data integrity refers to different measures taken to protect the content of the message and its accuracy; and availability refers to the accessibility of information by authorized users [6-8]. Furthermore, to guarantee the effectiveness of these security components, two additional features are required, namely authentication, which verifies the identity of the user, and authorization, which ensures that the user has the right to perform the tasks they wish to perform within the system [7]. To secure and protect sensitive medical information in connected healthcare systems, several mitigation measures have been implemented and others have been proposed. Examples include data encryption, use of cryptographic keys, biometrics and implementation of system-wide frameworks based on technologies such as Blockchain and X-Road [9-11]. These security measures are being used in systems that are not 5G-based. The 5G architecture is designed to be widely distributed and decentralized, allowing the public to have more access to the system through the use of cloud-based storage and processing servers, sensors, and smart phones[12]. 5G systems are expected to be the main drivers for the adoption of smart healthcare systems, thus enabling distributed and decentralised smart healthcare system architectures requiring new security solutions such as Blockchain and X-Road whose architectures are decentralized and distributed.

Although these security measures have shown potential to improve the delivery of smart healthcare by ensuring the security of data, there are still many security risks that cause vulnerabilities in smart healthcare systems. These include denial of service attacks performed on processing and storage servers, reverse engineering attacks[13] - a process by which a device is deconstructed to reverse its initial design, bots - a malicious software installed on mobile or medical devices for stealing medical information, eavesdropping on wireless or wired communication links and unauthorized access to data[14]. Attackers target vulnerabilities in these systems, and the attacks on health systems can have serious physical, social, and economic effects, and can potentially result in patient deaths [15].

This study aims to systematically review literature about security issues in emerging smart healthcare systems, with a focus on the security requirements, potential security risks, the measures currently being proposed to mitigate these risks, and the effectiveness of these measures. Preliminary results of the systematic literature review are presented.

A thorough examination of recent research was piloted, and we found that, Hameed et al. [16] conducted a systematic review on the security and privacy of Internet of Medical Things (IoMT) and their respective solutions by using machine learning techniques. Authors found that Machine learning techniques have been considerably deployed for device and network layer security; however, most studies barely represented IoMT systems.

Similarly, Liao et al. [17] performed a systematic review to analyse the security of IoT devices using mobile computing. Their systematic review only focussed on mobile computing particularly smart phones and therefore disregarded all other IoT based devices such as medical devices.

The main motivation that led to pursue this research was due to the strong security need for smart healthcare systems which was encouraged by the above gaps found in recent related work. Therefore, this necessitates for a systematic review to be conducted on studies that focuses on the security and privacy of smart healthcare systems which encompasses the Internet of medical things.

The main research question for the systematic review is: what are the security issues related to the acquisition, transmission, storage and sharing of patient health data in in Smart Healthcare systems? The systematic reviews aims to answer the following sub-questions: (a) What are the security requirements for secure acquisition, transmission, storage and sharing of patient health data in networked Smart Healthcare systems, (b) What are the security risks during the acquisition, transmission, storage and sharing of patient health data in networked Smart Healthcare systems, (c) What solutions have been proposed in literature to mitigate these security risks (d) How effective are the proposed security solutions.

II. METHODOLOGY

The review strategy used in this systematic review is the PICO, i.e., problem, intervention, comparator and outcome (PICO) systematic review search strategy. The problem addressed in this study is how to ensure the security and privacy of patient data smart healthcare systems. The intervention is the security measures that have been proposed to address the problem. The comparator is not applicable for this systematic review because this review focuses on the security measures available and in this case the comparator intervention is non-existent. The outcome is improved security in smart healthcare systems for patient data during acquisition, storage and while in transit.

The strategy included assessment of the security requirements for smart healthcare systems and the security measures that have been proposed to ensure the privacy and security of health data. The study also assessed the effectiveness of the proposed security measures in improving the security of patient data sharing, storage, and access. The systematic review has been registered with PROSPERO (the International Prospective Register of Systematic Reviews). This study has also adhered to PRISMA guidelines, an evidence-based set of items that aim to assist researchers improve the reporting of systematic reviews and meta-analyses [18]. PRISMA focuses on ways in which authors can ensure the complete and transparent reporting of systematic review studies [19]. The study is not restricted to any geographical setting.

The process and results of the study selection process was supported by the PRISMA flowchart shown in Fig. 1. The systematic review involved an exhaustive search of databases including Scopus, PubMed, Web of Science, Medline, CINAHL, Ebscohost and the Cochrane Library. Throughout the search only 3 databases yield results: Scopus, Web of science and Medline. The key search words and was carried out to identify studies that addressed the problem of security in smart healthcare systems and proposed solutions. The process of study selection was conducted with the use of the inclusion and exclusion criteria as shown in Table 1.

TABLE I
INCLUSION AND EXCLUSION CRITERIA TABLE

Characteristic	Inclusion Criteria	Exclusion Criteria
Problem	Articles on security in smart healthcare systems for patient data sharing, storage, acquisition and access control.	Articles that do not focus on health-related topics are excluded.
Intervention	Studies focusing on the security mechanisms used to mitigate against data breaches in smart healthcare systems.	Articles that do not demonstrate data protection during acquisition, transmission, storage, access and sharing are excluded.
Outcome	Studies that show improved security of smart healthcare systems for patient data sharing, storage, sharing and access control.	Studies that did not demonstrate end-to-end security in smart healthcare systems data sharing, storage and access control were excluded.

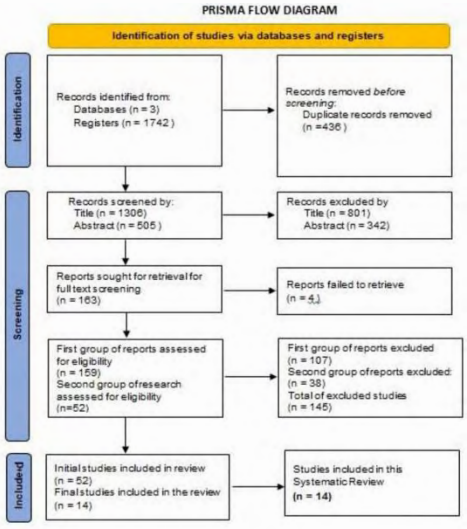

Figure 1: The PRISMA flowchart

III. FINDINGS AND RESULTS

Studies were screened for relevance using the study titles and abstracts, and consideration was given only to studies that addressed the problem of security in smart healthcare systems. The Final screening was carried out by reading full texts of the studies, and their relevance was defined by the reported PICO characteristics in each study. Excluded articles included those articles that did not focus on health-related topics, and articles that did not demonstrate end-to-end security in smart healthcare.

This systematic review identified a total of 1742 records through an exhaustive and comprehensive search from three electronic databases. Before performing screening, 436 records were identified as duplicates and they were removed. Using titles and abstracts, the remaining 1306 studies (after removing duplicates) were screened focusing on studies relating to the security of smart healthcare systems. From these 1306 articles, 801 records were excluded as they did not report security or smart healthcare system in their title, leaving a total of 505 articles. These 505 were further

screened based on their abstracts and 342 records were excluded after abstract screening leaving a total of 163 articles. Of the remaining 163 full texts, 4 records could not be found in all databases, at the University of Cape Town library, or even after contact the authors who were unreachable. Hence the remaining 159 full text articles were screened for eligibility. Of these 159 potentially eligible studies, 107 were initially excluded based on publication type such as analysis papers; and study focus such as studies focusing on the design of a system rather than its security. This initially led to 52 studies being eligible for inclusion in the study.

After further analysis by both reviewers, the remaining 52 studies were reassessed to focus the scope of this systematic review on end-to-end security. In order to be considered for inclusion, these studies needed to focus on improved end-to-end security in smart healthcare systems for patient data sharing, storage and access control. This led to the exclusion of 38 studies which were mostly focussing solely on wireless body area network as well as authentication and disregarded all other security requirements, i.e. these studies were not focussed on end-to-end security. A total of 14 studies were included in this systematic review.

1) Analysis based on research questions

The studies were classified into different subsections and analysed while trying to answer the research questions as follow:

a) What are the security requirements for networked Smart Healthcare systems?

First analysis was conducted based on security requirements stated in the studies. This question intended to provide a solution towards identifying different security requirements that are relevant for the full functionality of smart healthcare systems. Studies reported a number of security requirements that the proposed smart healthcare systems need to ensure the security of patient data. Studies reported the same security requirements i.e. confidentiality, integrity, availability, authorisation and authentication. These security requirements guide innovators when designing and implementing security measures that can provide robustness against data breaches.

Some examples of implemented security measures to meet the confidentiality security requirement were user registration, login and authentication phase to verify the user's identity thus ensuring that only authorised users have access to the system (3) (9) (11) (12) (13) (14). In some of the proposed solutions (1) (5) (7) (8) (10); the system needed to verify and validate the collected raw data and compare it to encrypted data stored in the cloud and the system had to follow some security procedures such as a mutual authentication between users and sensors according to secret keys generated to ensure the security, integrity and accessibility of data in the system Other studies have demonstrated that through the implementation of authentication schemes, several security features are enabled between patients, devices and healthcare providers to allow resilience to possible attacks by integrating anonymous authentication services (2) (4) (6). Likewise, blockchain technology can be used in smart healthcare systems to provide the protection of medical data and guarantees user authentication, integrity and confidentiality. It also ensures the protection, availability and allows data integrity preservation as blockchain keeps record of system access and user accountability. Hence the need for compatibility between the healthcare devices with the block chain technology in order to maintain the security of medical data (4).

b) What are the security risks in networked Smart Healthcare systems?

This question intended to identify reported security risks which could potentially result in the violation of the security of patient data.

The main security risk reported by several studies is the risk to confidentiality of data. These included eavesdropping in wireless communication mediums, and impersonation attacks. Secondly, the risk to the integrity of data was reported. These included data fabrication attack and message modification attack. i.e. modification of a patient's data and replacing it with incorrect data. Thirdly, other security risks reported were threat to the availability of data through denial-of-service attack (3) (9) (11) (12) (13) (14).

These reported security risks have the potential to cause harm to the patient, the data, and the healthcare system as a whole. A number of studies reported potential of security risks which are different attacks that could be launched to cause harm to patient's data, network, or the healthcare system such as authentication vulnerabilities, data security, access and privacy issues, data sharing and transmission issues as well as malware attacks (1) (5) (7) (8) (10). An example is when there is an unauthorised access to patient's data which happens when the attacker attempts to modify patient's data and replaces it with incorrect data. Consequently, incorrect data could lead to misdiagnosis which may affect patient health (10).

c) What solutions have been proposed in literature to mitigate these security risks?

Thirdly, studies reported different types of mitigation measures. For studies that focused on the security issues, such as end-to-end security as well as access control in EHR integrated into IoT; Authors reported solutions such as a security framework used for isolation of patient health data using network slicing techniques and user authentication (3). An end-to-end security scheme for IoT healthcare was proposed in order to provide end-to-end security from data acquisition, transmission access on servers and sharing of data (9). Three-tier hierarchical m-health system architecture has been proposed. It has a sensor network tier to collect patient's vital signs, a mobile computing network to process and route the data and a back-end network tier to analyse patient's medical data (11). Additionally, Authors proposed a healthcare system framework which is designed for data collection, data storage and data transmission through a wireless network infrastructure and published using a security gateway (12). A secure and privacy-preserving protocol for health data processing in mobile healthcare network is proposed for patient's data privacy (13). Cloud-based encryption architecture is proposed, it uses three types of encryption techniques: Advanced data encryption, Attribute-based encryption as well as proven data possession (14).

Moreover, studies that focused on data integrity and privacy of EHRs reported solutions such an architecture which combines biometric-based blockchain technology with the EHR system (2); A security model is proposed that allows protection of medical data using blockchain technology (4); as well as an innovative user cantered data sharing solution using blockchain technology (6).

Furthermore, studies focused on data sharing, exchange and transmission over the network in smart healthcare systems reported solutions such as symmetric encryption keys to encrypt the wireless communication from medical devices by avoiding wireless key exchange (1); An efficient data sharing scheme is proposed (MedChain). This Scheme uses block chain technology, peer-to-peer network and digests chain to overcome efficiency issues (5). Additionally, (7) proposed a trustworthy access control mechanism is achieved with the use of smart contracts to achieve security of EHR amongst patients and healthcare providers. A secure data transmission method using a complex encryption transmitting healthcare related data over the network by devices with resource constraint, as well as prevention of EHR modification by a third party (8); and finally, (10) an IoT-based smart healthcare security model framework is proposed to help design security areas for IoT services.

d) How effective are the proposed security solutions?

Included studies have demonstrated the effectiveness of the proposed mitigation measures in securing smart healthcare systems. These measures have shown potential to mitigate attacks in the systems and provide security protection. The effectiveness is guaranteed through the provision of security to patient's data and devices as well as the hospital devices. Some examples of reported the effectiveness are described below.

An end-to-end security as well as access control in EHR integrated into IoT reported the effectiveness as follows: The proposed security framework is shown to be effective by isolating the health traffic from general traffic. This is achieved through the implementation of a healthcare network slice reserved for caregivers and healthcare personnel. As well as a smart home network slice that provides connectivity to the elderly home (3). Another proposed security framework is shown to be effective by providing 97% more energy efficiency and was 10% faster. Authors also reported that the session redemption approach has 8.1% and 98.7% improvement on client-side and processing time respectively (9). Furthermore (11) reported that the system architecture has demonstrated its effectiveness using stochastic geometry, by showing how the transmitter is able to communicate with its neighbours with a higher average secrecy probability without the need of secure protocols such as RF Fingerprinting. The transmitter was able to extend its secure communication range by learning user's behaviour and trustworthiness. Also, being equipped with information on possible eavesdropping attack, the system is able to better perform in terms of secrecy and latency. Likewise, (12) proposed a healthcare system framework and reported its effectiveness in three areas. Namely, it uses easily deployed and low-cost wireless sensor networks, addresses the issue of achieving a direct communication between user's mobile and embedded medical devices, and also, it allows the enforcement of privacy preserving strategies and attains satisfactory performance. Hence, the proposed framework provides a significant component of the informationization of medical industries. Alex, et al. (13) reported that the proposed security framework was effective by through a comparison to Meshram's scheme described in the study; in terms of resource consumed and computational energy conception needed for access check depending on the number of users. Authors reported that as the number of helpers increases in the system, the required resources in requesting user's smart devices are reduced. Hence, the proposed protocol drastically reduces user's resource consumption and therefore decreases the resource conception ratio. And finally, (14) reported that the proposed security measure was shown to be effective by its ability to check and validate whether data is correctly encrypted and stored in the system. This is done by comparing the encrypted data stored in the cloud to the raw data input using advanced encryption methods such as attribute-based encryption, advanced encryption standards and provable data possession method. Authors concluded that this has resulted in an increase in data security, privacy and integrity; security and lower processing power.

Additionally, studies that focused on data integrity and privacy of EHRs such as (2), reported the effectiveness by comparing the use of secret and private keys to the proposed use of biometric based mechanism such as fingerprints. This proposed mechanism allows reduction in computational overhead required from patients, compared to the use of secret keys. The use of fingerprints also shows effectiveness in providing better audit logs for activities in the system and therefore analyses and prevents unauthorized activities; and provides a much more secure exchange and synchronization of the HER among healthcare providers. Also, (4) the security model security model is shown to be effective by evaluating the system performance based on its scalability and efficiency in data processing. The results shows that with a range of 10 to 10 000 requests, the system showed the average of 4.27 seconds response time with 10 0000 requests simultaneously. Also, regarding user permission grant/denial, the system responded with an average of 4.13 seconds response time per 10 000 user request simultaneously (grant) and 2.35 seconds response time (denial). Authors concluded that with these results, users can effectively manage the access to their data, as the system has demonstrated the ability to support high load of requests. This allows the system to perform transactions in a very effective way by granting and denying permissions to the rest of the participants. Then (6) demonstrated the effectiveness of the proposed solution by measuring its performance in terms of scalability and efficiency. With the focus on proof generation, data validation and data integrity, the system tested a number of concurrent records and concluded that it could handle s large data set at low latency. This indicates the effectiveness in scalability and efficiency of data.

Other studies focused on data sharing, exchange and transmission over the network in smart healthcare systems such as (1); reported that the proposed security framework is shown to be effective by analysing and testing the random

key generation. The key generation is tested based on two points. Namely, the stop-time in the system which is unknown to the adversary, and the number of iterations needed to produce the key. This leads to obtaining different key values resulting to a drastic sequence change of the generated key. Authors demonstrated that the security and randomness in the generated keys is achieved by using the proposed encryption technique. Hence the security of the encrypted message that is communicated between devices is achieved. (5) Showed how the proposed scheme MedChain was effective by analysing the system performance compared to existing blockchain-based solutions in terms of communication and storage overhead (5). The results show that in terms of the communication overhead in data access this approach facilitates integrity check in data access since it encodes the digest of data stream into a digest chain from blockchain and this allows validation of data integrity. Similarly, in terms of storage overhead, existing schemes stores all the data on the blockchain. However, for MedChain only stores the fingerprints and the rest of the data is stored on the directory servers which are mutable and the data can be removed from the servers only when the session is revoked. Hence MedChain guarantees less storage overhead.

Furthermore, (7) showed that the proposed system is shown to be effective by the author's performance analysis. Authors discuss that the proposed system is designed with its ability to provide flexibility as it is deployed on mobile platform and can be accessible to any authorize user with a smartphone. Additionally, authors measure the effectiveness of this system by its ability to provide high level of availability of health data anytime anywhere. They conclude that it uses a decentralized storage system which avoids single point of failure and also guarantees high security of data, integrity and privacy with the use of blockchain and smart contracts. (8) Measure the effectiveness by analysing the two-level encryption framework (Strong encryption done on the cloud and a light weight encryption done by the user) is shown to be effective by encrypting the whole image before sending it to the cloud, rather than the encryption of a portion of the image. This way, a lesser encryption time is achieved as compared to previous scheme such as the Saijjad scheme. To measure the effectiveness of the proposed framework in comparison to the Saijjad scheme, values of the encrypted data such as (Size of the compressed image, Pick signal ration, similarity index between old and new image and the number of changing pixel rate NPCR) should be as low as possible. Authors concluded that smaller values on the encrypted data was achieved, For example, I the case of medical image 1, Image dimensions were 256x256, when encrypting with the Saijjad scheme, the NPCR was 0.5784 and the proposed method yield the NCPCR of 0.6404. This method allows the preservation of the authenticity of the image as well as a lower encryption time, thus validating the effectiveness of the proposed encryption scheme. Finally, (10) demonstrated how the proposed security framework is shown to be effective by comparing the CPU and Memory performance with variation in the number of hosts in a network. The test results show that when the number of hosts is small, the CPU and Memory usage is high. However, as the number of hosts increases, the CPU and Memory usage does not increase linearly, but shows a small increase. This illustrated in the graph as follows: for memory usage, single system usage for 3 hosts is 12% and 11%; and for 8 hosts and 30% for 22% for distributed system. For CPU usage the figures are 6% and 7.8% for 3 hosts and 14% and 10% for 8 hosts.

IV. DISCUSSION AND CONCLUSIONS

The included articles described the smart healthcare system and identified the security requirements, security risks and solutions to mitigate the risks. Each study also explained the effectiveness of their proposed security solution. However, it was evident that some studies briefly reported the effectiveness of their proposed solution and this was considered poor reporting. Of the 14 studies included in the final selection, most of them focused on detecting security risks that have potential to cause harm to user authorization, data authentication, confidentiality, integrity and availability. However, while doing the study selection, it was evident that most of the excluded studies only focussed on user authorisation and authentication, hence they were excluded because they paid no attention to the rest of the security data journey which is securing data at the acquisition device, over the network while the data is being transferred as well as ensure the security of data at the storage device. Most studies have proposed measures such as biometrics, data encryption and blockchain technology to address security threats within the smart healthcare systems. These proposed measures have the potential to transform the security of smart healthcare systems and therefore to providing security of data from the point of acquisition, while being transferred through mobile networks, and during storage.

The limitation of this research is that it was carried upon a few selected online databases (3) namely Scopus, Medline and Web of Science due to other databases yielding result of 0 studies after the search queries were performed. Additionally, A few articles (4) could not be retrieved for full text analysis.

It is evident that the issue of securing data throughout its process from the acquisition, while being transferred through the network as well as at the storage has been resolved by providing end-to-end security of data. Studies have achieved this security by ensuring adherence to the proposed mechanisms. For example, by using the biometrics (fingerprints) mechanism for access control on the EHR, this eliminates the risk of permanent loss of identity and access control to EHRs and further assures patients data privacy (13). Another example is, with the use of a physical layer security scheme that was proposed for mobile computing tier in m-Health, patients medical data can be transferred with secrecy and delay constraints can be overcome (11). Also, by using MedChain, users exchange data through the blockchain technology which allows transaction of data without the need for a decentralized third party. This scheme is proven to provide efficient data sharing without any security compromise (5).

The results of the study are set to inform security system designers on the best approaches and policies for developing security mechanisms in smart healthcare systems. The results may also be useful to network operators in showing the potential risks to health information as it traverses mobile networks. The results could further be useful to conscientise