Format: Electronic Book

10th Global Conference on Cyber Security and Cloud Engineering 2023

Conference Proceeding

ISBN: 978-1-998259-09-0

Table of Contents

Content Details:

Parfaite Ndarhwa Nyamwezi (Author) *University of Cape Town*	**Security for Networked Smart Healthcare Systems: a Systematic Review**

Abstract

Smart healthcare systems use technologies such as wearable devices, Internet of Medical 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 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 analyze the concepts of interest. This study reviewed articles that have addressed end-to-end security risks in smart healthcare systems. It also 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. 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. This study concluded that 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 the protection of data in cases where the intruder has already accessed the system.

Keywords: PICO, 5G, mobile networks, security, smart health

Themes: Cyber Security Challenges in Different Sectors, Security and Integrity, Digital Privacy and Security.

1. 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. 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 focused 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.

2. 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 1. 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.

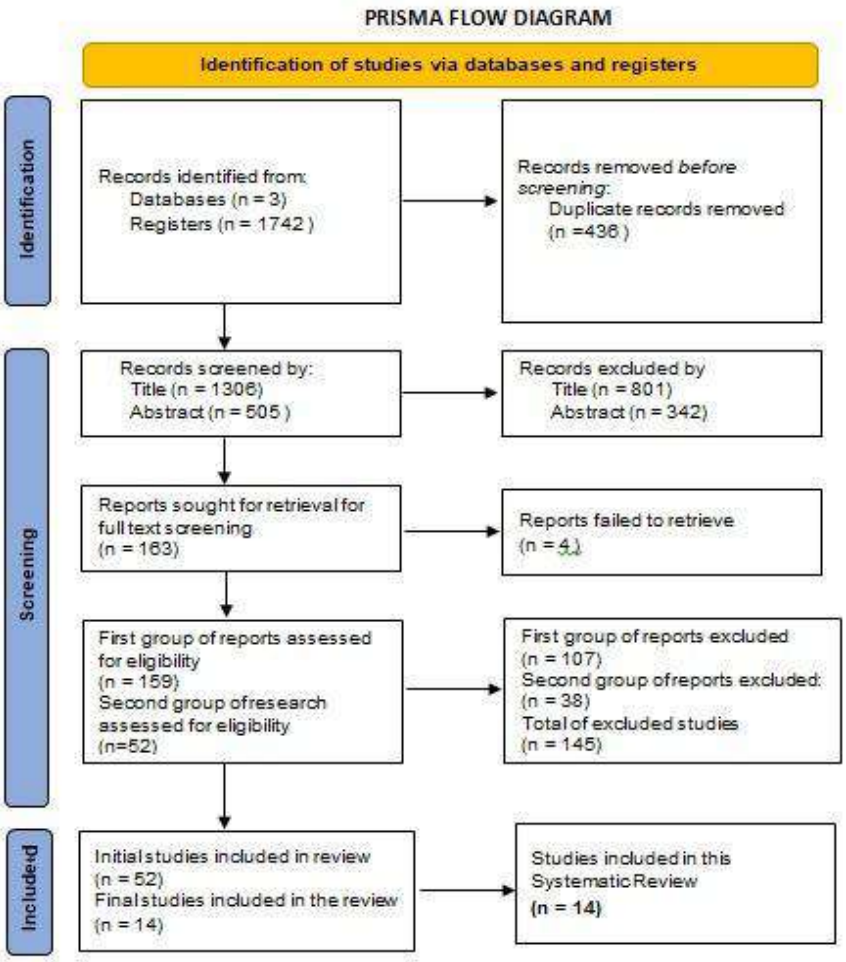

Figure 1. The PRISMA flowchart

3. 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.

3.1. **Analysis based on research questions**

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

3.1.1. 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).

3.1.2. 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).

3.1.3. 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.

3.1.4. 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.

4. 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 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.

References

[1]. Tian, S., et al., *Smart healthcare: making medical care more intelligent.* Global Health Journal, 2019. **3(3)**(3): p. 62-65.

[2]. Jagadeeswari, V., et al., *A study on medical Internet of Things and Big Data in personalized healthcare system.* Health Information Science and Systems, 2018. **6(1)**(1): p. 14.

[3]. Luna, R., et al., *Cyber threats to health information systems: A systematic review.* Technology and Health Care, 2016. **24(1)**(1): p. 1-9.

[4]. Ahmed, I., et al., *Wireless Communications for the Hospital of the Future: Requirements, Challenges and Solutions.* International Journal of Wireless Information Networks, 2020. **27**(1): p. 4-17.

[5]. Samaoui, S., et al., *Wireless and mobile technologies and protocols and their performance evaluation*, in *Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications*. 2015. p. 3-32.

[6]. Al-Janabi, S., et al., *Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications.* Egyptian Informatics Journal, 2017. **18(2)**(2): p. 113-122.

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

[8]. Tan, C.C., et al. *Body sensor network security: An identity-based cryptography approach*. in *WiSec'08: Proceedings of the 1st ACM Conference on Wireless Network Security*. 2008.

[9]. Ramli, S.N., et al. *A biometric-based security for data authentication in Wireless Body Area Network (WBAN)*. in *International Conference on Advanced Communication Technology, ICACT*. 2013.

[10]. Memon, Q.A. and A.F. Mustafa, *Exploring mobile health in a private online social network.* International Journal of Electronic Healthcare, 2015. **8(1)**(1): p. 51-75.

[11]. Malila, B. and T.E.M. Mutsvangwa, *Security architecture for a 5G mHealth system.* Global Health Innovation, 2019. **2(1)**(1): p. 1.

[12]. Mwangama, J., et al., *What can 5G do for healthcare in Africa?* Nature Electronics, 2020. **3(1)**(1): p. 7-9.

[13]. Imane, S., M. Tomader, and H. Nabil. *Comparison between CoAP and MQTT in Smart Healthcare and Some Threats*. in *International Symposium on Advanced Electrical and Communication Technologies, ISAECT 2018 - Proceedings*. 2019.

[14]. Kumar, P., et al. *Addressing a secure session-key scheme for mobility supported e-Healthcare systems*. in *International Conference on Advanced Communication Technology, ICACT*. 2014.

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

[16]. Hameed, S.S., et al., *A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches.* PeerJ Computer Science, 2021. **7**: p. 1-44.

[17]. Liao, B., et al., *Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review.* IEEE Access, 2020. **8**: p. 120331-120350.

[18]. Moher, D., et al., *Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement.* PLOS Medicine, 2009. **6**(7): p. e1000097.

[19]. Liberati, A., et al., *The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration.* PLoS Medicine, 2009. **6(7)**(7): p. 1000100.