World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

A survey of healthcare sector digitization strategies: Vulnerabilities, countermeasures and opportunities

Judith Nyakanga Nyakina [1,*] and Bahaa Hussein Taher [2]

[1] *Kenyatta National Hospital, Nairobi, Kenya.*
[2] *China University of Petroleum, Qingdao, China.*

World Journal of Advanced Engineering Technology and Sciences, 2023, 08(01), 282–301

Publication history: Received on 04 January 2023; revised on 17 February 2023; accepted on 20 February 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.8.1.0050

Abstract

The adoption of electronic healthcare in hospital environment can potentially reduce costs and improve the quality of life of the patients. However, numerous security and privacy issues arise when sensitive patient data is shared among multiple devices and users. Owing to its vulnerable nature, electronic health records seem to be more attractive to attackers compared to other forms of records such as financial transactions. Consequently, the patient data collected at the sensors, transmitted across communication channels and residing in hospital servers is susceptible to various threats. The goal of this paper was to carry out a survey of the electronic healthcare environment and attempt to understand the various weaknesses that can be exploited. This is followed by some descriptions of the various preventive mechanisms as well as the noted gaps. Therefore, numerous recommendations are given that are deemed fit for enhanced security and privacy posture in electronic healthcare domain.

Keyword: E-health; HER; Attacks; Security; Privacy

1. Introduction

The healthcare sector in most developing countries is facing a myriad of setbacks such as high costs, lack of public health systems, personnel and medications. The recent past has seen the rise in the incorporation of Information and Communication Technology (ICT) in the healthcare sector [1], creating an e-healthcare system. The goal is to enhance medical quality, data security and reduce costs. The utilization of ICT can therefore improve healthcare processes and facilitate remote health monitoring, more so in the rural areas. In this respect, smart medical devices, mobile devices and Internet of Things (IoT) offer remote patient monitoring. In this setting, IoT devices have embedded sensors that can establish connections over the internet and exchange information. Therefore, it becomes easy to control chronic ailments such as diabetes, high blood pressure and kidney diseases. These diseases are challenging for the healthcare system in terms of management and sustainability. However, with ICT incorporation, it becomes easier for doctors to offer assistance to patients in diverse phases such as diagnoses, monitoring and treatment. As explained in [2], IoT offers an infrastructure to facilitate the development of e-health systems. As shown in Figure 1, IoT provides tools such as sensors that collect vital patient physiological parameters such as heart rate, blood pressure and glucose level employed for remote monitoring for patients. In so doing, e-healthcare aid physicians to automate the process of medical signs collection and transmission so as to detect and report risk situations [3].

The continued usage of ICT in the healthcare sector has given rise to Internet of Healthcare Things (IoHT), Electronic Health Records (EHR) and Personal health record (PHR). Here, IoHT comprises of smart health devices that monitor, process, store and transmit sensitive information [4], [5]. A typical IoHT environment is characterized with uniquely identifiable devices, services, and software [6] as shown in Figure 2. These devices monitor patients by generating

*Corresponding author: Judith Nyakanga Nyakina

clinical data that is forwarded to remote servers over wireless communication channels. As such, the physicians and medical staff are able to remotely monitor their patients. IoHT also enable the patients to manage their health data with ease [7]. In so doing, IoHT offers efficient, reliable and cost effective healthcare services. On the other hand, PHR refers to an electronic application that enables individuals to access, manage and share their health information with parties that they authorize. This information exchange is executed in a secure, confidential and private environment [8]. On its part, EHR is the health sector's core digital strategy for enhancing the quality of care administered to patients. It accurately consolidates patient records from diverse healthcare providers over time [9] and shows the health status of the patients by checking their own EHR. Its adoption has led to the reduction of medical errors, enhancement of healthcare quality and minimization of costs [10], [11]. In so doing, it offers health education that fosters conscious decisions about health care [12].

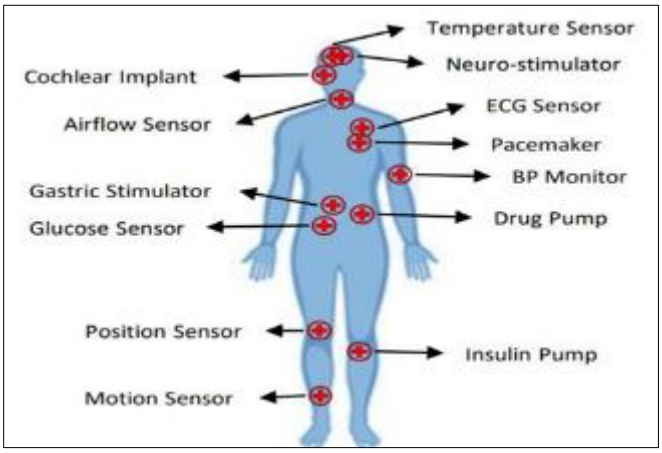

Figure 1 IoT body sensors [4]

Since EHR contains sensitive information, it is protected by law through the Health Information and Portability Accountability Association (HIPAA) [13]. It is clear that electronic health (E-health) has many promising outcomes in saving lives and hence has the potential of rapid adoption and expansion. Healthcare digitization offers reliability, efficiency, costs reductions, scalability and flexibility [14], [15], [16]. As pointed out in [17], many healthcare professional are considering it as part of the healthcare sector's future systems.

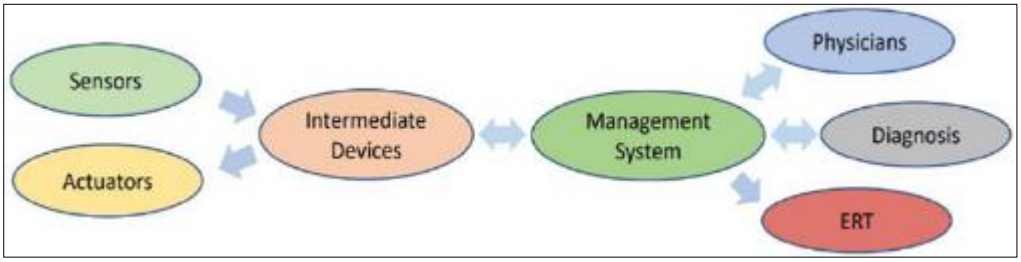

Figure 2 IoHT implementation [7]

Despite the many services offered by e-healthcare [18] systems, they face numerous challenges such as data privacy violations [4]. As such, there has been slower adoption of this digital transformation among healthcare organizations. Owing to the high volume and sensitive nature of patient records, the healthcare sector is cautious in the implementation of HER [19]. In addition, there have been reported cases of disrupted services, compromised health records, expensive payments to ransomware attackers, unavailability of essential health care services, and the stealing and selling of patient health records in the black market [20],[21]. During the COVID-19 pandemic, the big data held by the healthcare sector became a major target for ransom and attackers. As pointed out in [19], there has been an increase in the risks of attacks for non-optimal EHR implementations. For instance, there have been numerous high profile data breaches that have exposed EHR cyber security challenges. The authors in [22] explain that the limitations of IoT devices in terms of energy, computation and memory put constraints for the integration of IoT in healthcare. The mobility nature of IoT devices enables these devices to establish connections to the internet over different networks, hence affecting their security. As such, there has been slow adoption of IoHT in the healthcare sector despite the many investments from governments [23].This is also due to the sector's strict security and privacy requirements since it deals with human

lives. Therefore, safety is the top priority in healthcare organizations and they cannot risk adopting immature technology [24], [25].

The above issues point to the importance of deploying efficient security and privacy techniques to offer protection to e-healthcare systems from all threats [26], [27]. Privacy and security requirements such as integrity, confidentiality, authorization, authentication, non-repudiation and availability should be considered for IoT-healthcare applications [28]. As pointed out in [29], the protection of personal data from malicious entities and systems must be implemented at different levels such as processing, storage, communication and device levels. Although digital transformation is significant for the healthcare sector, susceptibility to cyber attacks is a fundamental challenge [30], [31], [32], [33].The general public trepidation towards e-healthcare is mainly due to privacy and security issues [30], [34]. Whereas privacy is concerned with the protection of the collected patients' data that can uniquely identify them, security is concerned with the restriction and authorization during access to this personal information [35]. In these healthcare systems, these two requirements are critical since leaked information has serious repercussions. As such, numerous cryptographic solutions have been proposed, which are geared towards data storage, privacy, access control, security and data ownership [36], [37]. The major contributions of this paper include the following:

- Extensive review of the electronic healthcare environment is provided so as to understand the various technological vulnerabilities that can be exploited by attackers.
- A survey of the various mechanisms challenges encountered during the sharing of the patient data are described
- The diverse techniques for privacy protection in an electronic healthcare domain are evaluated.
- The algorithms and protocols that have been developed for access control in e-health environment are studied and their weaknesses pointed out.
- A review of the techniques employed to protect stored data in patient IoT devices, hospital and cloud servers are analyzed.
- Some of the open research gaps are described so as to point out the possible research directions.

The rest of this article is structured as follows: Section 2 discusses the challenges in patient data sharing while Section 3 describes the various schemes for privacy protection. On the other hand, Section 4 analyses the diverse techniques for access control, while Section 5 discusses data storage security mechanisms. In Section 6, the key findings are reported while Section 7 points out some open research gaps. Finally, Section 8 concludes this paper and describes some future research scope.

2. Challenges in patient data sharing

Due to the continued enhancements in the digitization efforts in the healthcare sector, the volume of medical data is on the increase [38]. In this environment, sharing of patient electronic medical data becomes necessary to realize efficient integration of medical resources as well as improving medical staffs' diagnosis and treatment. Authors in [39], [40] explain that online diagnostic services offer analytics services to users at any time and place regarding real world healthcare services. However, medical data is sensitive and personal asset. This sharing increases the risks of data privacy leakages and abuses which pose major threats [41] to the lives and property of the patients. In this environment, interoperability is a key issue as it facilitates unified data exchange among researchers, patients and healthcare providers [42]. As pointed out in [43], medical data sharing promotes smart medicine but information systems heterogeneity among various medical institutions makes sharing difficult. In addition, sharing this sensitive medical data may lead to leakage of personal privacy [44].

Over the years, many IoT devices have been connected to the internet to store data on centralized servers. In this environment, the client-server architecture is employed to execute device connection, authorization and authentication. However, this architecture presents some challenges such as access control [45], single point of failure [46] and authentication. For instance, systems based on centralized communication with cloud servers [47] increases privacy and security risks [1]. On their part, authors in [48] explain that medical records in different formats are normally scattered among various medical institutions. This makes cumbersome to realize efficient data exchange and hence creating information islands. This curtails any efforts towards rapid, convenient, accurate diagnosis and treatment of the patients. This is supported by the authors in [49] who explain that contradictions exist regarding interoperability specifications of standard-based communication systems [50] as well as personal health devices. On their part, authors in [51] have pointed out that EHRs are vulnerable to numerous unauthorized accesses that violate privacy and data security. In addition, ransomware targeting e-health systems are on the rise [52]. Unfortunately, the current privacy preserving schemes are insufficient in the provision of foolproof security especially in e-health cloud environment. Therefore, the health records in the cloud are exposed to risks posed by internal attackers who have authorized access.

These privileged insiders may include system administrators, key managers and database administrators [53], [54], [55]. Figure 3 gives an illustration on the common causes of data leakages in an IoHT environment.

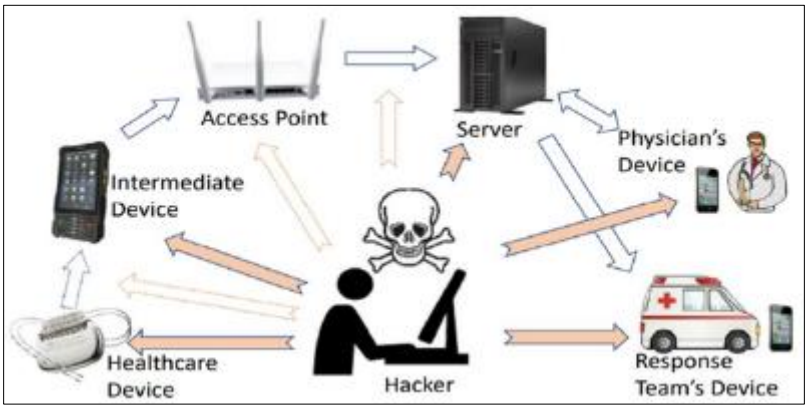

Figure 3 Sources of data leakages in IoHT environment [4]

The authors in [56] have explained the necessity of maintaining data privacy during the sharing of patient healthcare data. However, there are numerous challenges that crop up during the process of implementing privacy and security of telemedicine services. These challenges have continued to curtail the adoption of e-health services in most developing countries [57]. This can be explained by the adverse consequences that any successful security and privacy breach can have in these telemedicine services [58]. The risks are exponentially increased when the underlying telemedicine infrastructure is susceptible to security threats due to weak security measures [59], [60]. In addition, some ethical and legal issues may crop up in telemedicine services when proper authorization techniques are not put in place [61], [62]. In the preservation of semantic and structural integrity during the exchange of digital health data, heterogeneity has been cited in [63] to be a major problem. The current solutions to these challenges center around log analysis, access control, identity authentication and cryptography [64]. Unfortunately, these approaches are only concerned with the upholding of security and privacy of patient data but lack transparency guarantee during data access.

To address the issues above, many schemes and models have been developed to address these challenges. For instance, the authors in [65] have presented an application model to address interoperability issues in PHR. On the other hand, blockchain technology [66] has been cited in [67], [68], [69] to have crucial role in developing efficient and secure systems that can help resolve majority of the ethical and security issues in telemedicine services. For instance, blockchain can connect heterogeneous systems and offer authenticity as well as integrity guarantees for medical data sharing [43]. This position is supported by the authors in [70] who point out that there have been increasing attempts to deploy blockchain technology in the healthcare industry to address many of the EHR issues. Apart from this technology numerous regulatory standards have been created to protect sensitive patient data from being disclosed as well as enhance effectiveness and efficiency in the healthcare system. One of these standards is the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA privacy rule has helped create national standards that help protect patient data. Specifically, it offers a set of rules that uphold privacy and security of health information during its transfer, reception, handling and sharing. In addition to HIPAA, some necessary measures need to be incorporated in e-health systems to secure EHRs. These measures revolve around audit trails, data encryption and access control.

3. Schemes for privacy protection

The network architecture in e-health involves different entities. For instance, telemedicine systems comprise of diverse entities that must ensure the privacy of user data is maintained [71]. Data privacy is regarded as a fundamental requirement for e-health acceptance. To uphold data privacy, various approaches such as authentication, data flow representation as well as the authorization of the executed actions. These actions may include data collection, retention, processing and transmission. Unfortunately, many malicious activities might compromise the privacy of the users. Such activities may include unauthorized collection, usage, access, storage and sharing of the highly sensitive patient data. To protect against personal data leakages occasioned by these activities, suitable protection and security measures are needed [72], [73], [74], [75]. In addition, there is need for IoHT systems to be transparent to patients while at the same time providing updated information to ensure the protection of patients' data. To this end, a ubiquitous patient health record framework is presented in [76] to enable first-time patients to communicate their healthcare data to the medical providers. On the other hand, a privacy-preserving encryption [77] scheme is developed in [78] for medical data transmission and classification. On their part, the authors in [79] have presented an Attribute-Based Encryption (ABE)

and Identity-Based Encryption (IBE) scheme to encrypt data and hence facilitating fine-grained access control. However, identity based schemes are vulnerable to key escrow issues [80]. To solve these challenges, blockchain technology has been cited in [81] to be capable of improving data security and privacy. This is attributed to the ability of blockchain to offer security and data immutability through decentralization and cryptography [82] as shown in Figure 4.

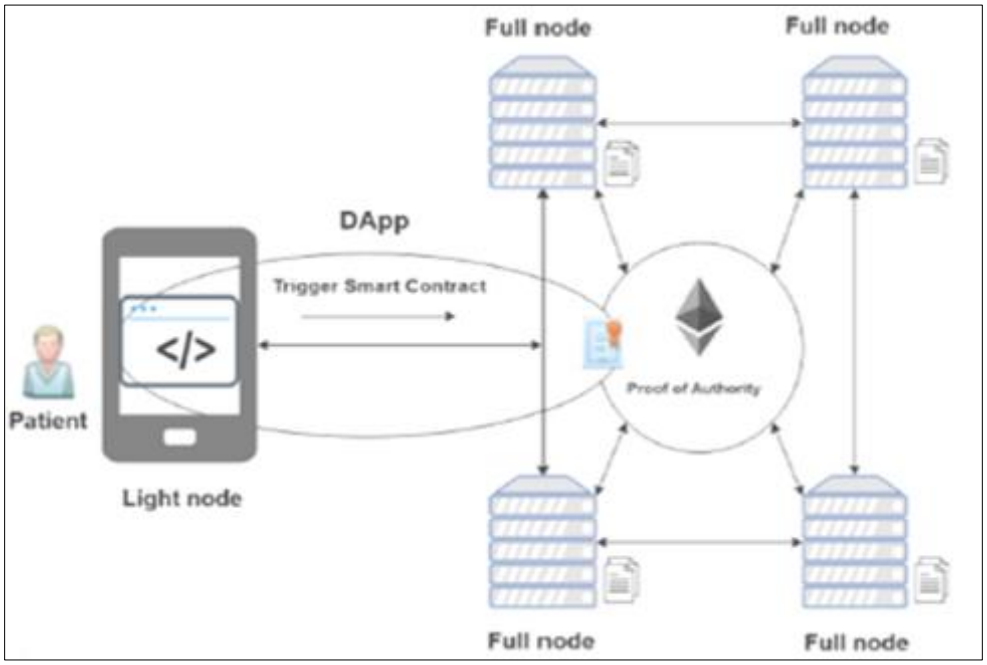

Figure 4 Patient interaction models in blockchain environment [4]

For instance, a blockchain based patient data transparent framework is developed in [83] to facilitate electronic medical record authorization management through the analysis [84] of the generated log events. Similarly, a blockchain based scheme is introduced in [85] to facilitate data encryption and storage in the local cloud. Using the consortium blockchain, authors in [43] have presented a medical data sharing scheme that achieves effective attribute-based access control [86], [87]. On the other hand, the Ethereum blockchain based solution in [88] has been shown to help in secure storage of EHR data. To offer optimized and intelligent medical data exchange among various entities, a medical-edge-blockchain scheme is developed in [89]. On the other hand, a Multi-Authority Attribute-Based Signatures (MA-ABS) based technique is developed in [68] to uphold privacy of patients. Similarly, a Hyperledger Fabric is introduced in [90] to conceal the identity of patients.

To boost privacy preservation and data security [91], encryption and proxy re-encryption technologies are amalgamated in [92] and implemented on Ethereum with the help of cloud storage [93], [94], [95], [96]. On the other hand, blockchain technology has been deployed in [97] and [70] to improve accuracy and efficiency [98] through effective medical data sharing among different institutions. Similarly, a data sharing management system based on the blockchain is presented in [99], while a blockchain based framework for patient-centered records and exchange is introduced in [100]. To improve security and privacy preservation [101] during electronic medical record sharing, a blockchain based approach is introduced in [102], while a lightweight backup recovery scheme for the medical blockchain key is developed in [103] to offer efficient [104] privacy protection. On the other hand, a blockchain based distributed model is developed in [65] to permit patient data to be interconnected between health organizations. To facilitate verifiability, privacy, auditability and data sharing, a decentralized medical record management system is introduced in [105]. Similarly, a privacy-preserving e-health system is presented in [106] to facilitate medical data exchange and speedy retrieval, while a blockchain-based data sharing framework for electronic medical records is developed in [107]. To offer data access control, tracing [108] and auditing, an effective medical record management system is presented in [109]. On the other hand, a blockchain based scheme is developed in [110] for secure image transmission and diagnoses. On the flip side, the blockchain technologies in [83], [89], [97], [70], [99], [102], [103], [106], [107], [109] has high space and computation complexities [111].

4. Techniques for access control

In an e-health environment, the patients have complete control when it comes to granting and revoking access to their medical records [112], [113]. This helps preserve confidentiality of the health data. In addition, encryption has been cited in [78] to be an effective means of secure transmission of medical data over public network.For instance, a blockchain-based e-health integrity model is developed in [114] to boost information integrity. Similarly, a blockchain-based architecture is introduced in [115] to ensure availability, security [116], confidentiality and integrity of patient records. This architecture also supports secure international, cross-institutional and internal exchange of health records. To permit authenticated users to access the record for a particular session, authors in [117] have developed a public-key cryptography based scheme for the encryption of the data in the off-chain storage [118]. On the other hand, a decentralized platform for tracking and exchanging patients' health records is developed in [119]. To enhance confidentiality through encryption of medical data being stored on the cloud, authors in [120] have developed elliptical curve [121] certificateless aggregate cryptography signature scheme. Through encryption, this scheme is demonstrated to prevent forgery of medical data blocks, while the secure certificateless public auditing scheme facilitates the checking of data using an auditor.

To facilitate confidential medical data sharing in a multi-authority cloud storage environment, cloud storage, [122] and attribute-based signcryption (ABSC) algorithm are deployed. Similarly, a general framework for sharing critical EHR records is introduced in [123]. Here, access control and encryption are employed to uphold the confidentiality of the health records [124]. To ensure proper authentication in EHR solutions, a data aggregation scheme and group authentication based on blockchain technology is developed in [125]. Here, the group session key [126] is deployed by multiple authorized users such as patients, doctors, caregivers, family and friends to freely access the patient's encrypted private information [127]. On the other hand, a multi-agent based distributed ledger system is developed in [128] to enhance EHR security. Similarly, a Hyperledger Fabric blockchain based access control management system is introduced in [129] for emergency medical situations, while a blockchain-based system for securing IoT devices in the healthcare environment is developed in [1].

To facilitate the secure sharing of medical image, a blockchain [130] based scheme is introduced in [131], while a fine-grained access control system is developed in [132] to improve data privacy and security. Here, all access management processes are executed on the blockchain. Therefore, these processes are logged in a transparent and traceable manner.To facilitate medical data sharing devoid of intermediaries, a novel medical data processing architecture is developed in [133]. This approach is demonstrated to prevent data leakage risks that may be occasioned by improper operation during processing. Similarly, a fine-grained access control scheme for medical records [134] is introduced in [112] based on the blockchain. Here, the medical records are stored in the cloud and proxy re-encryption is utilized for data sharing [135]. On the other hand, a user-centric medical record sharing solution is developed in [136] based on blockchain technology Hyperledger Fabric [137]. This system is shown to preserve privacy and prevent any vulnerability during data storage. Similarly, authors in [138] have developed an architecture that facilitates electronic medical record sharing based on the Hyperledger. This system also implements an access control using symmetric key cryptography to enhance data accessibility between healthcare providers. On their part, the authors in [139] have developed a blockchain based framework that facilitates fine-grained access control [140] and keyword search in the decentralized storage systems.

An electronic medical record architecture is presented in [141] to offer fine-grained access authorization while at the same time maintaining compatibility with blockchain. Similarly, a technique based on blockchain and smart contract is developed in [142] to enable healthcare centers to securely share their encrypted HER. To attain secure search, data security, privacy protection and access control, a personal health information sharing scheme is introduced in [143] based on blockchain technology. Unfortunately, the schemes in [129], [131], [133], [136], [138], [139], [141], [142] and [143] have high space and storage complexities [144]. As such, a lightweight secure and privacy preserving scheme for ECG diagnoses and visualization is presented in [145].

5. Secure storage mechanisms

The continued deployment of IoHT has led to corresponding increase in the need for cost-effective data storage. As such, many approaches have been presented in literature over the recent past. For instance, a scheme that uses symmetric and asymmetric key cryptography is introduced in [146] for secure data storage. Here, one smart contract is employed to store the mapping between the patient, combined key and the hash values, while another smart contract is utilized by patients to control the granting and revoking of access. To offer security for health and medicinal data in cloud based IoT platform, a remote health-monitoring technique is presented in [147]. In this approach, a lightweight [148] block

encryption technique is deployed to offer the required protection. On the other hand, a blockchain based data preservation system is developed in [149] for medical data. Here, the blockchain architecture is deployed to provide verifiability and primitiveness of saved data as well as preserving the client privacy. Similarly, a hybrid of data encryption modules is introduced in [150] to protect diagnoses data in medicinal images, while a holistic on-chain and off-chain collaborative storage system is developed in [151] for efficient storage [152] and verification of EHR data [153]. On the other hand, a hash table based scheme is introduced in [154] for medical data storage and retrieval from the cloud. Here, the EHR data is enciphered using the blockchain's hash function so as to preserve its confidentiality [155]. On their part, their authors in [156] introduce a novel steganography system to protect stored records, while a technique for encrypting medical images is developed in [157]. Similarly, a scheme to secure mobile healthcare network data is presented in [158], while a technique to protect stored medical data is introduced in [159]. Here, users are able to send and receive encrypted data [160] from a wearable devices [161]. This is unlike an approach in [162] where the emphasis was on secure sharing of health data in the digital healthcare system [163], [105], [164].

On the other hand, a secure, low cost, scalable and tamper-proof health data sharing system is developed in [165]. This approach is shown to solve numerous challenges problems that blockchain-based technologies have faced. On their part, authors in [166] have extended the framework in [161] by developing a General Data Protection Regulation (GDPR) compliant proof-of-concept system that is shown to facilitate efficient [167] and secure health data exchange. On the other hand, the authors in [168] have developed a consent management system to uphold availability of data to concerned parties. In addition, this system offers scalability and integrity of the data. Similarly, a secure and scalable solution is presented in [169] which is based on Ethereum blockchain technology. On their part, the authors in [170] have presented blockchain architecture for storing health records to address privacy and accessibility challenges of patients' records. This approach is shown to ensure data privacy and accessibility. To store the states of access control to patient data, a state machine is introduced in [171], in which the three states include access policy, individual authorization state and record life cycle. On their part, Ethereum blockchain based protocol is developed in [172] to enable the IoT sensors to communicate securely with smart contract implemented smart device.

6. Key Findings

It is evident that healthcare has evolved significantly over the recent past due to the adoption of ICT in healthcare processes such as data collection, storage, diagnostics, and treatment [159]. The emergence of the industrial internet of things (IIoT) has advanced e-health by facilitating the development of connected healthcare systems that enhance interoperability, visibility and data connectivity. However, the deployment of such technology has led to growing concerns regarding security and privacy [173] of healthcare data. The risks are further increased when the collection, sharing and processing is accomplished via cutting-edge connected sensor devices. It has also been noted that EHRs systems have been deployed in many healthcare environments, where the technological advancements have revolutionized access control, storage and processing of health data [174]. However, digital health information may lead to misinterpreted health information due to unreliable data, which could put a patient's life at risk [175].Similarly, it has been observed that unauthorized third-party access to health data collected by smart devices and wearable devices might put sensitive information at risk. As such, quality and validated medical devices, smart-phones, and sensors [176] are needed to offer accurate health data to the participants [177].

It has been established that EHR systems have numerous benefits that have positively impacted the healthcare sector. However, there are also many security and privacy challenges that affect development of e-Health [178] and hence have curtailed the deployment of existing e-health systems [179]. Since these systems collected sensitive information [180] whose leakage might effect the patient's life and social status [181], proper security and privacy protection should be provided. As explained in [182], health records digitization has lead to an array of attacks such as privileged inside, denial of service and information leakages. Therefore, organizations have to setup guidelines for the administration of healthcare information so as to achieve the desired level of security and privacy. In this context, security ensures that authorized access is granted to only those parties with rights to access health information [183]. Therefore, availability, integrity and confidentiality of medical data are advocated here. Particularly, confidentiality ensures that sensitive information such as medical history, behavior problems and various patient issues are kept secret. This ensures that illegal access which can affect the mental and physical health of a patient is prevented. It is also important that accuracy and correctness be upheld for e-health systems so as to ensure that this data is free from faults.

Regarding stored data, the significance of confidentiality, integrity, and privacy concerns have been stressed in [184] and [185]. Over the recent past, blockchain has appeared to be a secure [186] and decentralized platform and hence can address some of these issues. As pointed out in [187], this technology has greatly changed the storing and sharing of health data by promoting security and accuracy of the data whilst reducing maintenance cost [188]. Here, patient medical data are stored in a distributed manner, devoid of full access to that medical data [189]. However, there are

certain limitations to blockchain technology such as high storage complexities. It has also been noted that IIoT has become a disruptive computing paradigm across various domains such as smart cities [190], [191], [192], healthcare [193], [194], [195] and manufacturing [196], [133]. It has introduced ubiquity in the sharing of healthcare data [197] and therefore transforming healthcare from digital to intelligent [198]. This has greatly improved the quality of healthcare services. However, this paradigm is plagued with numerous privacy and security challenges [199]. For instance, the usage of wearable and embedded devices for diagnostic and treatment procedures is increasingly common [200], [201], raising concerns about privacy and security of patient data. It is therefore common for the healthcare data to become an attractive target for cyber attacks.

It has been revealed that the data sent by IoT devices generally do not follow any end-to-end encryption and decryption scheme. Worse still, patient data are shared across diverse tiers of the healthcare system and hence attaining security and privacy of such data is a challenge task [200], [201]. In this environment, any disruptions in transfer, update or sharing of data can lead to exposure of patient data [202], [203]. For instance, authors in [204] have pointed out that cyber security breaches in health data is considered more lucrative than credit cards on the illegal market due to their life-threatening nature. In this environment, distributed ledger technologies such as Bitcoin can be deployed to facilitate decentralized data collection and processing in a tamper-proof manner [205], [206], [207], [208]. However, the deployment of blockchain in IoHT is inefficient to a number of factors [209]. To start with, the transparency in blockchain means that all patient data is visible to everyone on blockchain [210], [211], [212]. Obviously, this leads to leakage of the highly sensitive [213] personal medical records. Another challenge is that of scalability and speed since blockchain transactions are very long. For instance, authors in [214] explain that for a transaction to be final on the blockchain, it has to wait for 6 blocks to be added to the longest chain. This means that blockchain solutions cannot be applicable in medical emergency scenarios [188]. Moreover, the blockchain can be expensive to implement [215], [216] since a node has to pay some fees for the transactions.

7. Open research gaps

It has been shown that the e-health environment is characterized with confidential and sensitive data that may include social security number and credit card details. Therefore, any successful compromise can leak sensitive person data and cause some financial losses. Although many techniques have been put forward to prevent data leakages, many challenges still exist. For instance, the attribute -based encryption (ABE) techniques are ineffective due to their costly computations. As explained in [217], issues such as effective access control, authentication, key management efficient user revocation, secure storage and data encryption are yet to be addressed. To address some of these problems, IoT-related data privacy protection policies, protocols [218] and frameworks have been developed for user privacy and data protection. However, these frameworks and policies are yet to attain intended results. Therefore, healthcare data privacy protection is insufficient [73]. It has also been shown that some limitations exist of the current healthcare data privacy laws in that they fail to offer a particular set of instructions to protect IoHT data.

To address the shortcomings in the existing IoHT devices' operating systems, specialized operating systems such as Contiki, RIOT, TinyOS and FreeRTOS have been developed [219]. However, the constrained nature of IoT devices in terms of power, memory and computation still renders them vulnerable to the system and network attacks. This is because complex encryption and authentication schemes cannot be implemented in these resource constrained devices. As such, it is easy for attackers to employ memory vulnerabilities to compromises the security of such devices [220]. The literature reviewed has shown that the blockchain technology offers salient features such as autonomy, transparency, anonymity, openness as well as decentralized, unforgeable and tamper resistance EHR protection. In so doing, it helps address challenges of poor reliability, low security, low efficiency and high costs associated with current centralized security models. In light of these challenges, the following recommendations are critical in resolving healthcare data security and privacy problems.

7.1. Complete anonymization of health records

In a typical e-health environment, the IoT devices gather and aggregate data from various patients before fording it to the router or any intermediary device for further processing. During this process, compression technique are deployed to minimize storage requirements especially for big headers like Internet Protocol IPv6 header. To prevent privacy leaks, these records should be anonymized such that tracing them to their owner becomes tricky.

7.2. Penalties and fines for privacy leaks

High volumes of data are collected and processed by IoHT devices and hence privacy risks are always inherent regarding access and usage of this data. For instance, behavior monitoring and individual identification are serious issues. As such, entities that maliciously perform these activities must be penalized with heavy fines.

7.3. Sufficient laws and guidelines

In IoT healthcare domain, several communication protocols have been developed. However, there are no particular guidelines provided in data privacy laws regarding protocol security. There is also lack of guidelines concerning the encryption type or anonymity standards to be adopted in IoT devices. There is therefore need for privacy laws that offer transparent policies regarding communication security of these devices, especially for hospital usage.

7.4. User friendly designs

The controls in healthcare system should be designed in such a manner that they are user-friendly. The patients should also be able to have full control over their collected data at any moment. This means that the controls should enable the patient to decide whom to share or not to share the data with. The controls should also allow the patients to know who has their data, what data has been collected and for which purpose is the data intended.

7.5. Education and awareness

The awareness programs are crucial for management staff, IT staff and other relevant healthcare facility staff so as to highlight the importance of data privacy. All these parties should be aware of secure processing of healthcare data, as well as the consequences of data leakages. In addition, they should be familiar with the penalties they would be charged in the case of carelessness. This education and awareness should involve secure usage of staff devices such as laptops and cell-phones that are linked to healthcare systems. For instance, authors in [221] explain that despite concerted efforts in executing e-health ideas and projects, many of these efforts have failed to satisfactorily reach their goals due to lack of awareness among the population.

7.6. Embed privacy in the designs

The system developers should strive to implement privacy safeguard framework in the e-healthcare infrastructure from the beginning of the system engineering process. Conventionally, the e-healthcare devices operate through user interactions or web interfaces where there are no privacy protection guidelines dictating how device interfaces should be designed. In addition, numerous vulnerabilities lurk in web-based interfaces which can be exploited to cause data leakages and information leakage attacks. Unfortunately, most of the devices lack authentication features, while other have default passwords which are cumbersome to input due to their small size interfaces.

7.7. Interoperable data protection laws

Although there are various data privacy laws, their enforcement varies regionally and internationally. This presents some challenges when healthcare data of citizens are processed in a different country or state where different data privacy laws are enforced. This is to do with the possible legal issues that should apply to that citizen's processed data.

8. Conclusion

This paper sought to offer some survey on the vulnerabilities, threats and exploits in an electronic health domain. In addition, the various security solutions implemented during patient data sharing, storage and collection are discussed. The findings have indicated that the e-health environment is characterized by numerous threats and vulnerabilities that can be exploited by attackers. As a matter of fact, numerous attacks have already been perpetrated in this domain, leading to serious privacy leaks and financial losses. As such, many security solutions have been developed. Therefore, this paper provided some review of these techniques upon which various weaknesses and performance issues were pointed out. In a nutshell, the attainment of perfect security in an e-health scenario is quite challenging. This can be explained by the many devices and users involved, as well as the limited computation and energy at the sensor devices. Therefore, various recommendations have been given in this paper, which are thought to be significant for the improvement of privacy in patient data handling. Future research may include the extensive study of the technical recommendations that have been provided so as to envision how they can be put into actual practice.

Compliance with ethical standards

Acknowledgments

We would like to thank our colleagues and relatives who supported us during the drafting and finalizing of this manuscript.

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Azbeg K, Ouchetto O, Andaloussi SJ. Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management. IEEE Transactions on Computational Social Systems. 2022 Jul 8.

[2] Al-Shaher MA, Al-Khafaji NJ. E-healthcare system to monitor vital signs. In2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) 2017 Jun 29 (pp. 1-5). IEEE.

[3] Andrès E, Talha S, Benyahia AA, Keller O, Hajjam M, Moukadem A, Dieterlen A, Hajjam J, Ervé S, Hajjam A. E-health: A promising solution for optimizing management of chronic diseases. Example of the national e-health project e-care based on an e-platform in the context of chronic heart failure. European Research in Telemedicine/La Recherche Européenne en Télémédecine. 2015 Sep 1, 4(3):87-94.

[4] Shahid J, Ahmad R, Kiani AK, Ahmad T, Saeed S, Almuhaideb AM. Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences. 2022 Feb 12, 12(4):1927.

[5] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Feb 8:103117.

[6] Ahmad T, Ranise S. Validating Requirements of Access Control for Cloud-Edge IoT Solutions (Short Paper). InFoundations and Practice of Security: 11th International Symposium, FPS 2018, Montreal, QC, Canada, November 13–15, 2018, Revised Selected Papers 11 2019 (pp. 131-139). Springer International Publishing.

[7] Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV. The quest for privacy in the internet of things. IEEE Cloud Computing. 2016 May 25, 3(2):36-45.

[8] Heart T, Ben-Assuli O, Shabtai I. A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. Health Policy and Technology. 2017 Mar 1, 6(1):20-5.

[9] Al-Zubaidie M, Zhang Z, Zhang J. PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system. International Journal of Environmental Research and Public Health. 2019 May, 16(9):1490.

[10] Vimalachandran P, Wang H, Zhang Y, Zhuo G. The Australian PCEHR system: ensuring privacy and security through an improved access control mechanism. arXiv preprint arXiv:1710.07778. 2017 Oct 21.

[11] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[12] Xu J, Gao X, Sorwar G, Croll P. Implementation of e-health record systems in Australia. The International Technology Management Review. 2013 Jul, 3(2):92-104.

[13] Alassaf N, Alkazemi B, Gutub A. Applicable light-weight cryptography to secure medical data in IoT systems. Arabia. 2003 Mar.

[14] Parviainen P, Tihinen M, Kääriäinen J, Teppola S. Tackling the digitalization challenge: how to benefit from digitalization in practice. International journal of information systems and project management. 2017, 5(1):63-77.

[15] McLoughlin IP, Garrety K, Wilson R. The digitalization of healthcare: Electronic records and the disruption of moral orders. Oxford University Press, 2017 Jan 19.

[16] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[17] Wernhart A, Gahbauer S, Haluza D. eHealth and telemedicine: Practices and beliefs among healthcare professionals and medical students at a medical university. PloS one. 2019 Feb 28, 14(2):e0213067.

[18] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct, 28(1):183-91.

[19] Pilares IC, Azam S, Akbulut S, Jonkman M, Shanmugam B. Addressing the challenges of electronic health records using blockchain and ipfs. Sensors. 2022 May 26, 22(11):4032.

[20] He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of medical Internet research. 2021 Apr 20, 23(4):e21747.

[21] Ferreira A, Cruz-Correia R. COVID-19 and cybersecurity: finally, an opportunity to disrupt?. Jmirx med. 2021 May 6, 2(2):e21069.

[22] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[23] Palas MJ, Bunduchi R. Exploring interpretations of blockchain's value in healthcare: a multi-stakeholder approach. Information technology & people. 2020 Jun 24, 34(2):453-95.

[24] Edmunds M, Peddicord D, Frisse ME. Ten reasons why interoperability is difficult. Healthcare information management systems: Cases, strategies, and solutions. 2016:127-37.

[25] Madsen LB. Data-driven healthcare: how analytics and BI are transforming the industry. John Wiley & Sons, 2014 Oct 27.

[26] Sahi MA, Abbas H, Saleem K, Yang X, Derhab A, Orgun MA, Iqbal W, Rashid I, Yaseen A. Privacy preservation in e-healthcare environments: State of the art and future directions. Ieee Access. 2017 Oct 30, 6:464-78.

[27] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan, 11(24):12040.

[28] Amaraweera SP, Halgamuge MN. Internet of things in the healthcare sector: overview of security and privacy issues. Security, privacy and trust in the IoT environment. 2019:153-79.

[29] Kumar JS, Patel DR. A survey on internet of things: Security and privacy issues. International Journal of Computer Applications. 2014 Jan 1, 90(11).

[30] Alassaf N, Gutub A. Simulating light-weight-cryptography implementation for IoT healthcare data security applications. International Journal of E-Health and Medical Communications (IJEHMC). 2019 Oct 1, 10(4):1-5.

[31] Offner KL, Sitnikova E, Joiner K, MacIntyre CR. Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intelligence and National Security. 2020 Jun 6, 35(4):556-85.

[32] Kheshaifaty N, Gutub A. Engineering graphical captcha and AES crypto hash functions for secure online authentication. Journal of Engineering Research. 2021 Nov 10.

[33] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[34] Papoutsi C, Reed JE, Marston C, Lewis R, Majeed A, Bell D. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. BMC medical informatics and decision making. 2015 Dec, 15:1-5.

[35] Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021 Jul 1, 22(2):177-83.

[36] Vimalachandran P, Wang H, Zhang Y, Heyward B, Zhao Y. Preserving patient-centred controls in electronic health record systems: A reliance-based model implication. In2017 International Conference on Orange Technologies (ICOT) 2017 Dec 8 (pp. 37-44). IEEE.

[37] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[38] Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. Health information science and systems. 2014 Dec, 2:1-0.

[39] Liang J, Qin Z, Xiao S, Ou L, Lin X. Efficient and secure decision tree classification for cloud-assisted online diagnosis services. IEEE Transactions on Dependable and Secure Computing. 2019 Jun 14, 18(4):1632-44.

[40] Ni J, Lin X, Shen XS. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. IEEE Journal on Selected Areas in Communications. 2018 Mar 12, 36(3):644-57.

[41] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. InArtificial Intelligence and Sustainable Computing: Proceedings of ICSISCET 2021 2022 Nov 16 (pp. 91-111). Singapore: Springer Nature Singapore.

[42] Hussein R, Crutzen R, Gutenberg J, Kulnik ST, Sareban M, Niebauer J. Patient-Generated Health Data (PGHD) Interoperability: An Integrative Perspective. InMIE 2021 May 27 (pp. 228-232).

[43] Zhang D, Wang S, Zhang Y, Zhang Q, Zhang Y. A secure and privacy-preserving medical data sharing via consortium blockchain. Security and Communication Networks. 2022 May 18, 2022.

[44] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[45] Yang Y, Wu L, Yin G, Li L, Zhao H. A survey on security and privacy issues in Internet-of-Things. IEEE Internet of things Journal. 2017 Apr 17, 4(5):1250-8.

[46] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Computer networks. 2013 Jul 5, 57(10):2266-79.

[47] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6). IEEE.

[48] Jin H, Luo Y, Li P, Mathew J. A review of secure and privacy-preserving medical data sharing. IEEE Access. 2019 May 14, 7:61656-69.

[49] Urbauer P, Sauermann S, Frohner M, Forjan M, Pohn B, Mense A. Applicability of IHE/Continua components for PHR systems: Learning from experiences. Computers in biology and medicine. 2015 Apr 1, 59:186-93.

[50] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[51] Chenthara S, Ahmed K, Wang H, Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access. 2019 May 30, 7:74361-82.

[52] Alzubi OA, Chen TM, Alzubi JA, Rashaideh H, Al-Najdawi N. Secure channel coding schemes based on algebraic-geometric codes over Hermitian curves. J. Univers. Comput. Sci.. 2016 Jan 1, 22(4):552-66.

[53] Alzubi JA, Alzubi OA, Suseendran G, Akila D. A novel chaotic map encryption methodology for image cryptography and secret communication with steganography. Int J Recent Technol Eng. 2019 May, 8(1C2):1122-8.

[54] Alzubi OA, Alzubi JA, Dorgham O, Alsayyed M. Cryptosystem design based on Hermitian curves for IoT security. The Journal of Supercomputing. 2020 Nov, 76:8566-89.

[55] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432).

[56] Pramanik PK, Pareek G, Nayyar A. Security and privacy in remote healthcare: Issues, solutions, and standards. InTelemedicine technologies 2019 Jan 1 (pp. 201-225). Academic Press.

[57] Hossain CA, Zishan MS, Ahasan DR. A review on the security issues of telemedicine network. Int J Innov Res Elect Electron Instrument Control Eng. 2014 Nov, 2:2183-85.

[58] Razali RA, Jamil N. A quick review of security issues in telemedicine. In2020 8th International Conference on Information Technology and Multimedia (ICIMU) 2020 Aug 24 (pp. 162-165). IEEE.

[59] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014, 16(5):137-44.

[60] Jalali MS, Landman A, Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association. 2021 Mar, 28(3):671-2.

[61] Kaplan B. Revisiting health information technology ethical, legal, and social issues and evaluation: telehealth/telemedicine and COVID-19. International journal of medical informatics. 2020 Nov 1, 143:104239.

[62] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[63] Chatterjee A, Pahari N, Prinz A. HL7 FHIR with SNOMED-CT to achieve semantic and structural interoperability in personal health data: a proof-of-concept study. Sensors. 2022 May 15, 22(10):3756.

[64] Jayabalan M, O'Daniel T. Access control and privilege management in electronic health record: a systematic literature review. Journal of medical systems. 2016 Dec, 40(12):261.

[65] Roehrs A, Da Costa CA, da Rosa Righi R. OmniPHR: A distributed architecture model to integrate personal health records. Journal of biomedical informatics. 2017 Jul 1, 71:70-81.

[66] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[67] Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. The role of blockchain technology in telehealth and telemedicine. International journal of medical informatics. 2021 Apr 1, 148:104399.

[68] Guo H, Li W, Nejad M, Shen CC. Access control for electronic health records with hybrid blockchain-edge architecture. In2019 IEEE International Conference on Blockchain (Blockchain) 2019 Jul 14 (pp. 44-51). IEEE.

[69] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9, 3(5):364.

[70] Mackey TK, Kuo TT, Gummadi B, Clauson KA, Church G, Grishin D, Obbad K, Barkovich R, Palombini M. 'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC medicine. 2019 Dec, 17(1):1-7.

[71] Buldakova TI, Sokolova AV. Network services for interaction of the telemedicine system users. In2019 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA) 2019 Nov 20 (pp. 387-391). IEEE.

[72] Solanas A, Patsakis C, Conti M, Vlachos IS, Ramos V, Falcone F, Postolache O, Pérez-Martínez PA, Di Pietro R, Perrea DN, Martinez-Balleste A. Smart health: A context-aware health paradigm within smart cities. IEEE Communications Magazine. 2014 Aug 7, 52(8):74-81.

[73] Eckhoff D, Wagner I. Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Communications Surveys & Tutorials. 2017 Sep 5, 20(1):489-516.

[74] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[75] Alghanim AA, Rahman SM, Hossain MA. Privacy analysis of smart city healthcare services. In2017 IEEE International Symposium on Multimedia (ISM) 2017 Dec 11 (pp. 394-398). IEEE.

[76] Kyazze M, Wesson J, Naude K. The design and implementation of a ubiquitous personal health record system for South Africa. Stud. Health Technol. Inform. 2014 Nov 14, 206:29-41.

[77] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[78] Alzubi JA, Alzubi OA, Beseiso M, Budati AK, Shankar K. Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis. Expert Systems. 2022 May, 39(4):e12879.

[79] Wang S, Zhang Y, Zhang Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. Ieee Access. 2018 Jun 29, 6:38437-50.

[80] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[81] Hossain CA, Mohamed MA, Zishan MS, Ahasan R, Sharun SM. Enhancing the security of E-Health services in Bangladesh using blockchain technology. International Journal of Information Technology. 2022 May, 14(3):1179-85.

[82] Shi S, He D, Li L, Kumar N, Khan MK, Choo KK. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & security. 2020 Oct 1, 97:101966.

[83] Jayabalan M, Thiruchelvam V. A design of patients data transparency in electronic health records. In2017 IEEE International Symposium on Consumer Electronics (ISCE) 2017 Nov 14 (pp. 9-10). IEEE.

[84] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1, 23(4):145-62.

[85] Jiang S, Wu H, Wang L. Patients-controlled secure and privacy-preserving EHRs sharing scheme based on consortium blockchain. In2019 IEEE Global Communications Conference (GLOBECOM) 2019 Dec 9 (pp. 1-6). IEEE.

[86] Dolev S, Krzywiecki Ł, Panwar N, Segal M. Vehicle authentication via monolithically certified public key and attributes. Wireless Networks. 2016 Apr, 22:879-96.

[87] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[88] Andola N, Prakash S, Venkatesan S, Verma S. SHEMB: A secure approach for healthcare management system using blockchain. In2019 IEEE Conference on Information and Communication Technology 2019 Dec 6 (pp. 1-6). IEEE.

[89] Abdellatif AA, Samara L, Mohamed A, Erbad A, Chiasserini CF, Guizani M, O'Connor MD, Laughton J. Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange. IEEE Internet of Things Journal. 2021 Jan 19, 8(21):15762-75.

[90] Stamatellis C, Papadopoulos P, Pitropakis N, Katsikas S, Buchanan WJ. A privacy-preserving healthcare framework using hyperledger fabric. Sensors. 2020 Nov 18, 20(22):6587.

[91] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[92] Wang Y, Zhang A, Zhang P, Wang H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. Ieee Access. 2019 Sep 23, 7:136704-19.

[93] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE access. 2019 May 17, 7:66792-806.

[94] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[95] Chen L, Lee WK, Chang CC, Choo KK, Zhang N. Blockchain based searchable encryption for electronic health record sharing. Future generation computer systems. 2019 Jun 1, 95:420-9.

[96] Cao S, Zhang G, Liu P, Zhang X, Neri F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences. 2019 Jun 1, 485:427-40.

[97] Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L. A systematic review of the use of blockchain in healthcare. Symmetry. 2018 Oct 10, 10(10):470.

[98] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1, 11(1):185-94.

[99] Kim MG, Lee AR, Kwon HJ, Kim JW, Kim IK. Sharing medical questionnaries based on blockchain. In2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM) 2018 Dec 3 (pp. 2767-2769). IEEE.

[100] Hylock RH, Zeng X. A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study. Journal of medical Internet research. 2019 Aug 31, 21(8):e13592.

[101] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[102] Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics. 2020 Feb 1, 134:104040.

[103] Zhao H, Bai P, Peng Y, Xu R. Efficient key management scheme for health blockchain. CAAI Transactions on Intelligence Technology. 2018 Jun, 3(2):114-8.

[104] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1, 13(1).

[105] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In2016 2nd international conference on open and big data (OBD) 2016 Aug 22 (pp. 25-30). IEEE.

[106] Zou R, Lv X, Zhao J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Information Processing & Management. 2021 Jul 1, 58(4):102604.

[107] Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information. 2017 Apr 17, 8(2):44.

[108] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[109] Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE access. 2017 Jul 24, 5:14757-67.

[110] Alzubi OA. A deep learning-based frechet and dirichlet model for intrusion detection in IWSN. Journal of Intelligent & Fuzzy Systems. 2022 Jan 1, 42(2):873-83.

[111] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec, 11(4):66.

[112] Thwin TT, Vasupongayya S. Blockchain-based access control model to preserve privacy for personal health record systems. Security and Communication Networks. 2019 Jun 25, 2019.

[113] Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A blockchain based privacy preserving platform for healthcare data. InSecurity, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10 2017 (pp. 534-543). Springer International Publishing.

[114] Hyla T, Pejaś J. eHealth integrity model based on permissioned blockchain. Future Internet. 2019 Mar 24, 11(3):76.

[115] Lee HA, Kung HH, Udayasankaran JG, Kijsanayotin B, B Marcelo A, Chao LR, Hsu CY. An architecture and management platform for blockchain-based personal health record exchange: development and usability study. Journal of Medical Internet Research. 2020 Jun 9, 22(6):e16748.

[116] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[117] Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos one. 2020 Dec 9, 15(12):e0243043.

[118] Hussien HM, Yasin SM, Udzir NI, Ninggal MI. Blockchain-based access control scheme for secure shared personal health records over decentralised storage. Sensors. 2021 Apr 2, 21(7):2462.

[119] Margheri A, Masi M, Miladi A, Sassone V, Rosenzweig J. Decentralised provenance for healthcare data. International Journal of Medical Informatics. 2020 Sep 1, 141:104197.

[120] Benil T, Jasper JJ. Cloud based security on outsourcing using blockchain in E-health systems. Computer Networks. 2020 Sep 4, 178:107344.

[121] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[122] Yang X, Li T, Xi W, Chen A, Wang C. A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud. IEEE Access. 2020 Sep 18, 8:170713-31.

[123] Demir O, Kocak B. A decentralized file sharing framework for sensitive data. InBig Data Innovations and Applications: 5th International Conference, Innovate-Data 2019, Istanbul, Turkey, August 26–28, 2019, Proceedings 5 2019 (pp. 142-149). Springer International Publishing.

[124] Liang Y. Identity verification and management of electronic health records with blockchain technology. In2019 ieee international conference on healthcare informatics (ichi) 2019 Jun 10 (pp. 1-3). IEEE.

[125] Li CT, Shih DH, Wang CC, Chen CL, Lee CC. A blockchain based data aggregation and group authentication scheme for electronic medical system. IEEE Access. 2020 Sep 22, 8:173904-17.

[126] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[127] Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE transactions on network science and engineering. 2019 Dec 25, 8(2):1242-55.

[128] Alruwaili FF. Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records. PeerJ Computer Science. 2020 Nov 30, 6:e323.

[129] Rajput AR, Li Q, Ahvanooey MT, Masood I. EACMS: Emergency access control management system for personal health record based on blockchain. IEEE Access. 2019 May 20, 7:84304-17.

[130] Nyangaresi VO, Khalefa MS, Abduljabbar ZA, Al Sibahee MA. Low Bandwidth and Side-Channeling Resilient Algorithm for Pervasive Computing Systems. InProceedings of International Conference on Communication and Computational Technologies: ICCCT 2022 2022 Sep 27 (pp. 193-208). Singapore: Springer Nature Singapore.

[131] Tang H, Tong N, Ouyang J. Medical images sharing system based on blockchain and smart contract of credit scores. In2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) 2018 Aug 15 (pp. 240-241). IEEE.

[132] Meier P, Beinke JH, Fitte C, Schulte To Brinke J, Teuteberg F. Generating design knowledge for blockchain-based access control to personal health records. Information Systems and e-Business Management. 2021 Mar, 19:13-41.

[133] Cheng J, Chen W, Tao F, Lin CL. Industrial IoT in 5G environment towards smart manufacturing. Journal of Industrial Information Integration. 2018 Jun 1, 10:10-9.

[134] Tariq F, Khan ZA, Sultana T, Rehman M, Shahzad Q, Javaid N. Leveraging Fine-Grained Access Control in Blockchain-Based Healthcare System. InAdvanced Information Networking and Applications: Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020) 2020 (pp. 106-115). Springer International Publishing.

[135] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[136] Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) 2017 Oct 8 (pp. 1-5). IEEE.

[137] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, Muralidharan S. Hyperledger fabric: a distributed operating system for permissioned blockchains. InProceedings of the thirteenth EuroSys conference 2018 Apr 23 (pp. 1-15).

[138] Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020 Feb 1, 50:102407.

[139] Wang H, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of medical systems. 2018 Aug, 42(8):152.

[140] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[141] Zhang X, Poslad S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In2018 IEEE International conference on communications (ICC) 2018 May 20 (pp. 1-6). IEEE.

[142] Wang M, Guo Y, Zhang C, Wang C, Huang H, Jia X. MedShare: a privacy-preserving medical data sharing system by using blockchain. IEEE Transactions on Services Computing. 2021 Sep 24.

[143] Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems. 2018 Aug, 42(8):140.

[144] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[145] Shaikh MU, Adnan WA, Ahmad SA. Secured electrocardiograph (ECG) signal using partially homomorphic encryption technique–RSA algorithm. Pertanika Journal of Science and Technology. 2020, 28(S2):231-42.

[146] Reen GS, Mohandas M, Venkatesan S. Decentralized patient centric e-Health record management system using blockchain and IPFS. In2019 IEEE Conference on Information and Communication Technology 2019 Dec 6 (pp. 1-7). IEEE.

[147] Akhbarifar S, Javadi HH, Rahmani AM, Hosseinzadeh M. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. Personal and Ubiquitous Computing. 2020 Nov 16:1-7.

[148] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep, 33(9):e4528.

[149] Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-based data preservation system for medical data. Journal of medical systems. 2018 Aug, 42:1-3.

[150] Pushpa B. Hybrid data encryption algorithm for secure medical data transmission in cloud environment. In2020 Fourth international conference on computing methodologies and communication (ICCMC) 2020 Mar 11 (pp. 329-334). IEEE.

[151] Sun Y, Zhang R, Wang X, Gao K, Liu L. A decentralizing attribute-based signature for healthcare blockchain. In2018 27th International conference on computer communication and networks (ICCCN) 2018 Jul 30 (pp. 1-9). IEEE.

[152] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[153] Miyachi K, Mackey TK. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information processing & management. 2021 May 1, 58(3):102535.

[154] El Sayed AI, Abdelaziz M, Megahed MH, Azeem MH. A new supervision strategy based on blockchain for electronic health records. In2020 12th International Conference on Electrical Engineering (ICEENG) 2020 Jul 7 (pp. 151-156). IEEE.

[155] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[156] Pandey HM. Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. Future Generation Computer Systems. 2020 Oct 1, 111:213-25.

[157] Denis R, Madhubala P. Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications. 2021 Jun, 80:21165-202.

[158] Sun X, Zhang P, Sookhak M, Yu J, Xie W. Utilizing fully homomorphic encryption to implement secure medical computation in smart cities. Personal and Ubiquitous Computing. 2017 Oct, 21:831-9.

[159] Abdullah S, Arshad J, Khan MM, Alazab M, Salah K. PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle. Complex & Intelligent Systems. 2022 Jan 21:1-9.

[160] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[161] Brogan J, Baskaran I, Ramachandran N. Authenticating health activity data using distributed ledger technologies. Computational and structural biotechnology journal. 2018 Jan 1, 16:257-66.

[162] Bartolomeu PC, Vieira E, Ferreira J. IOTA feasibility and perspectives for enabling vehicular applications. In2018 IEEE Globecom Workshops (GC Wkshps) 2018 Dec 9 (pp. 1-7). IEEE.

[163] Gropper A. Powering the physician-patient relationship with HIE of one blockchain health IT. InONC/NIST use of Blockchain for healthcare and research workshop. Gaithersburg, Maryland, United States: ONC/NIST 2016 Aug 7.

[164] Divya M, Biradar NB. IOTA-next generation block chain. Int. J. Eng. Comput. Sci. 2018 Apr, 7(04):23823-6.

[165] Zheng X, Sun S, Mukkamala RR, Vatrapu R, Ordieres-Meré J. Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. Journal of medical Internet research. 2019 Jun 6, 21(6):e13583.

[166] Hawig D, Zhou C, Fuhrhop S, Fialho AS, Ramachandran N. Designing a distributed ledger technology system for interoperable and general data protection regulation–compliant health data exchange: A use case in blood glucose data. Journal of medical Internet research. 2019 Jun 14, 21(6):e13665.

[167] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25, 4(1):10-9.

[168] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. InAMIA annual symposium proceedings 2017 (Vol. 2017, p. 650). American Medical Informatics Association.

[169] Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for eHealth data access management. In2017 fourth international conference on advances in biomedical engineering (ICABME) 2017 Oct 19 (pp. 1-4). IEEE.

[170] Flavio da Conceição A, Soares Correa da Silva F, Rocha V, Locoro A, Marcos Barguil J. Eletronic Health Records using Blockchain Technology. arXiv e-prints. 2018 Apr:arXiv-1804.

[171] Dias JP, Sereno Ferreira H, Martins Â. A blockchain-based scheme for access control in e-health scenarios. InProceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018) 10 2020 (pp. 238-247). Springer International Publishing.

[172] Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems. 2018 Jul, 42:1-7.

[173] Nyangaresi VO, Abduljabbar ZA, Mutlaq KA, Hussain MA, Hussien ZA. Forward and Backward Key Secrecy Preservation Scheme for Medical Internet of Things. InHuman-Centric Smart Computing: Proceedings of ICHCSC 2022 2022 Nov 29 (pp. 15-29). Singapore: Springer Nature Singapore.

[174] Sahama T, Simpson L, Lane B. Security and Privacy in eHealth: Is it possible?. In2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013) 2013 Oct 9 (pp. 249-253). IEEE.

[175] Fahy E, Hardikar R, Fox A, Mackay S. Quality of patient health information on the Internet: reviewing a complex and evolving landscape. The Australasian medical journal. 2014, 7(1):24.

[176] Plante TB, Urrea B, MacFarlane ZT, Blumenthal RS, Miller ER, Appel LJ, Martin SS. Validation of the instant blood pressure smartphone app. JAMA internal medicine. 2016 May 1, 176(5):700-2.

[177] Hekler EB, Buman MP, Grieco L, Rosenberger M, Winter SJ, Haskell W, King AC. Validation of physical activity tracking via android smartphones compared to ActiGraph accelerometer: laboratory-based and free-living validation studies. JMIR mHealth and uHealth. 2015 Apr 15, 3(2):e3505.

[178] Haque ME, Ahsan MA, Rahman F, Islam A, EmdadulHaque M. The challenges of ehealth implementation in developing countries: a literature review. IOSR Journal of Dental and Medical Sciences. 2019 May, 18(5):41-57.

[179] Pussewalage HS, Oleshchuk VA. Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management. 2016 Dec 1, 36(6):1161-73.

[180] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 569-574). IEEE.

[181] Ghazvini A, Shukur Z. Security challenges and success factors of electronic healthcare system. Procedia Technology. 2013 Jan 1, 11:212-9.

[182] Coppolino L, D'Antonio S, Mazzeo G, Romano L. Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering. 2017 Apr 1, 59:126-40.

[183] Domínguez-Mayo FJ, Escalona MJ, Mejías M, Aragón G, García-García JA, Torres J, Enríquez JG. A strategic study about quality characteristics in e-health systems based on a systematic literature review. The Scientific World Journal. 2015 Jan 1, 2015.

[184] Bleikertz S, Schunter M, Probst CW, Pendarakis D, Eriksson K. Security audits of multi-tier virtual infrastructures in public infrastructure clouds. InProceedings of the 2010 ACM workshop on Cloud computing security workshop 2010 Oct 8 (pp. 93-102).

[185] Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. IEEE Security & privacy. 2010 Jun 17, 9(2):50-7.

[186] Nyangaresi VO, Ma J, Al Sibahee MA, Abduljabbar ZA. Packet Replays Prevention Protocol for Secure B5G Networks. InProceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 2 2022 Jul 27 (pp. 507-522). Singapore: Springer Nature Singapore.

[187] Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJ. BHEEM: A blockchain-based framework for securing electronic health records. In2018 IEEE Globecom Workshops (GC Wkshps) 2018 Dec 9 (pp. 1-6). IEEE.

[188] Radanović I, Likić R. Opportunities for use of blockchain technology in medicine. Applied health economics and health policy. 2018 Oct, 16:583-90.

[189] Badr S, Gomaa I, Abd-Elrahman E. Multi-tier blockchain framework for IoT-EHRs systems. Procedia Computer Science. 2018 Jan 1, 141:159-66.

[190] Hammi B, Khatoun R, Zeadally S, Fayad A, Khoukhi L. Internet of things (iot) technologies for smart cities, IET Networks 7, 2017.

[191] Samih H. Smart cities and internet of things. Journal of Information Technology Case and Application Research. 2019 Jan 2, 21(1):3-12.

[192] Rajab H, Cinkelr T. IoT based smart cities. In2018 international symposium on networks, computers and communications (ISNCC) 2018 Jun 19 (pp. 1-4). IEEE.

[193] Nyangaresi VO, Al Sibahee MA, Abduljabbar ZA, Ma J, Khalefa MS. Biometric-Based Packet Validation Scheme for Body Area Network Smart Healthcare Devices. In2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON) 2022 Jun 14 (pp. 726-731). IEEE.

[194] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 1, 29(7):1645-60.

[195] Alansari Z, Soomro S, Belgaum MR, Shamshirband S. The rise of Internet of Things (IoT) in big healthcare data: review and open research issues. Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2016, Volume 2. 2018:675-85.

[196] Tao F, Zuo Y, Da Xu L, Zhang L. IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE transactions on industrial informatics. 2014 Feb 17, 10(2):1547-57.

[197] Bashshur RL, Shannon G, Krupinski EA, Grigsby J. Sustaining and realizing the promise of telemedicine. Telemedicine and e-Health. 2013 May 1, 19(5):339-45.

[198] Zheng X, Rodríguez-Monroy C. The development of intelligent healthcare in China. Telemedicine and e-Health. 2015 May 1, 21(5):443-8.

[199] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Temporary Symmetric Key Based Message Verification Protocol for Smart Energy Networks. In2022 IEEE 7th International Energy Conference (ENERGYCON) 2022 May 9 (pp. 1-6). IEEE.

[200] Hwang YH. Iot security & privacy: threats and challenges. InProceedings of the 1st ACM workshop on IoT privacy, trust, and security 2015 Apr 14 (pp. 1-1).

[201] Rayes A, Salam S, Dabbagh M, Rayes A. Internet of things security and privacy. Internet of Things From Hype to Reality: The Road to Digitization. 2017:195-223.

[202] Chacko A, Hayajneh T. Security and privacy issues with IoT in healthcare. EAI Endorsed Transactions on Pervasive Health and Technology. 2018 Jul 23, 4(14).

[203] Butt SA, Diaz-Martinez JL, Jamal T, Ali A, De-La-Hoz-Franco E, Shoaib M. IoT smart health security threats. In2019 19th International conference on computational science and its applications (ICCSA) 2019 Jul 1 (pp. 26-31). IEEE.

[204] Sadek I, Rehman SU, Codjo J, Abdulrazak B. Privacy and security of IoT based healthcare systems: concerns, solutions, and recommendations. InHow AI Impacts Urban Living and Public Health: 17th International

Conference, ICOST 2019, New York City, NY, USA, October 14-16, 2019, Proceedings 17 2019 (pp. 3-17). Springer International Publishing.

[205] Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017 Nov 1, 24(6):1211-20.

[206] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. InCognitive Radio Oriented Wireless Networks and Wireless Internet: 16th EAI International Conference, CROWNCOM 2021, Virtual Event, December 11, 2021, and 14th EAI International Conference, WiCON 2021, Virtual Event, November 9, 2021, Proceedings 2022 Mar 31 (pp. 325-340). Cham: Springer International Publishing.

[207] Angraal S, Krumholz HM, Schulz WL. Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes. 2017 Sep, 10(9):e003800.

[208] Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal. 2018 Jan 1, 16:224-30.

[209] Dave E. How the next evolution of the internet is changing everything. The Internet of Things. 2011 Apr:2011.

[210] Kan L, Wei Y, Muhammad AH, Siyuan W, Gao LC, Kai H. A multiple blockchains architecture on inter-blockchain communication. In2018 IEEE international conference on software quality, reliability and security companion (QRS-C) 2018 Jul 16 (pp. 139-145). IEEE.

[211] De Filippi P. The interplay between decentralization and privacy: the case of blockchain technologies. Journal of Peer Production, Issue. 2016 Sep 14(7).

[212] Seo J, Park M, Oh H, Lee K. Money laundering in the bitcoin network: Perspective of mixing services. In2018 International Conference on Information and Communication Technology Convergence (ICTC) 2018 Oct 17 (pp. 1403-1405). IEEE.

[213] Nyangaresi VO, Abduljabbar ZA, Abduljabbar ZA. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC) 2021 Dec 20 (pp. 188-193). IEEE.

[214] Mamoshina P, Ojomoko L, Yanovich Y, Ostrovski A, Botezatu A, Prikhodko P, Izumchenko E, Aliper A, Romantsov K, Zhebrak A, Ogu IO. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget. 2018 Jan 1, 9(5):5665.

[215] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In2017 IEEE international congress on big data (BigData congress) 2017 Jun 25 (pp. 557-564). Ieee.

[216] Lamtzidis O, Pettas D, Gialelis J. A novel combination of distributed ledger technologies on internet of things: Use case on precision agriculture. Applied System Innovation. 2019 Sep 18, 2(3):30.

[217] Gönen S, Sayan HH, Yılmaz EN, Üstünsoy F, Karacayılmaz G. False data injection attacks and the insider threat in smart systems. Computers & Security. 2020 Oct 1, 97:101955.

[218] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Abood EW, Abduljaleel IQ. Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids. InAd Hoc Networks and Tools for IT: 13th EAI International Conference, ADHOCNETS 2021, Virtual Event, December 6–7, 2021, and 16th EAI International Conference, TRIDENTCOM 2021, Virtual Event, November 24, 2021, Proceedings 2022 Mar 27 (pp. 188-204). Cham: Springer International Publishing.

[219] Chung, B., Kim, J., Jeon, Y. On-demand security configuration for IoT devices. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 19–21 October 2016, pp. 1082–1084.

[220] Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of things Journal. 2018 Jun 15, 6(2):1606-16.

[221] Hossain CA, Mohamed MA, Zishan MS, Ahsan R, Sharun SM. Awareness on E-Health among undergraduate students in Bangladesh. Indian J Public Health Res Dev. 2019 Mar 1, 10:636-41.