Review

Analysis of Blockchain in the Healthcare Sector: Application and Issues

Ammar Odeh [1], Ismail Kesha [2], and Qasem Abu Al-Haija [3,*]

[1] Computer Science Department, Princess Sumaya University for Technology, Amman, Jordan; a.odeh@psut.edu.jo
[2] Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia, imohamed@mcst.edu.sa
[3] Computer Science/Cybersecurity Department, Princess Sumaya University for Technology, Amman, Jordan; q.abualhaija@psut.edu.jo
* Correspondence: q.abualhaija@psut.edu.jo (Q.A.A-H)

Abstract: The emergence of blockchain know-how currently presents the opportunity for the health sector to adopt such technologies in electronic health records. Blockchain assists in maintaining and sharing the relevant medical records of the patient with the relevant group of healthcare providers and the hospital. Numerous specific applications include traceability of drug and patient monitoring or Electronic Health Records (EHR). While Blockchain assists in maintaining and sharing the relevant medical records of the patient with the relevant group of healthcare providers and the hospital, it is important to note that the moral consciousness of the healthcare professionals is the main guide of the moral consciousness is ethics. This paper presents an overview of the application of blockchain in the healthcare and medical sector, highlighting the specific challenges and concerns. The study adopted a systematic review of secondary literature in answering the research question.

Keywords: Blockchain; Healthcare; Privacy; Cybersecurity; Healthcare-records

1. Introduction

Healthcare is an important sector for both the developed and upcoming nations. This is specifically attributed to the fact that healthcare is the only sector concerned directly with the general social wellbeing and lives of members of the population. Scholarly studies and development within the health sector have been an ongoing process as the world aims to improve its population's overall quality of life [1]. With the development and recent advancement in innovations, the improvement witnessed within the health industry can be noticed without much struggle. The overall capabilities of the medical and healthcare sector have been improved further by initiating innovative and latest computer technologies within the sector. Such advancements in computer technologies may help physicians and other relevant health providers with the timely diagnosis and management of numerous health-related problems [5]. Different revolutionary and emerging computer technologies have since been applied within other sectors with the highly promising outcome. Such technologies comprise the Internet of Things, Blockchain, Data Mining, Cloud Computing, and the Internet of Things, Blockchain, Data Mining, Cloud Computing, and Internet of Things, Blockchain Data Mining, Cloud Computing, and many others [22].

As Ratta et al. (2021) [2] described, Blockchain is a point-to-point distributed network within which no single third party has been involved in the communication and transaction. All the undertakings are isolated and not linked to other relevant transactions. For instance, the popular innovatory idea of cryptocurrency is supported by blockchain technology [13]. Similarly, cryptocurrency is highly believed to be very much secured and not able to be hacked; the same blockchain concept can be applied in other sectors to enhance security and privacy issues. The healthcare sector is one of the relevant industries where the technology can effectively be applied.

Within the blockchain, a ledger system that is publicly distributed is accessible to any individual. In this case, blockchain e is the list of records that keep the required information sequentially. In' this case, the block is the container with all the details of the individual transaction. The block has both the header and the details of the transaction. The header is responsible for keeping all the information related to the block [6]. With its associated security features, Blockchain can easily be into the healthcare system to enhance the effectiveness of the 'sector's operations. The present paper seeks to establish how Blockchain can be applied in the healthcare sector, highlighting the specific challenges and concerns.

1.1 Our objectives

To present an overview of the application of Blockchain in the healthcare sector, highlighting the specific challenges and concerns. Specifically, As per the broad objectives, the study seeks to achieve the following specific objectives.

- To establish how blockchain technology can be applied to improve the general performance of the medical sector
- To explore the various challenges and concerns of the application of Blockchain in the healthcare system

2. Materials and Methods

2.1. Study design

The research focused on the specific research topic by developing a systematic review of viable secondary literature. Torres-Carrión PV (2018) [32] argues that a vast amount of data exists pertinent to medical data encryption. Carrying out the present research using existing secondary data is achievable. A more extensive definition of a secondary literature review entails interpreting and analyzing data that other groups of researchers previously collected. The viability of the research approach arises from the cost and time savings because it does not encompass going to the field to collect data. The term desk top review arises from the ease with which researchers can review data at the desktop. Resource and time availability determined how the researcher selected the approach. Secondary data is easily accessible and assists the researcher in illustrating the problems with clear and better insight. The study guaranteed that the information application was accurate, current, and relevant.

2.2 Sampling procedure

Secondary literature sampling involves picking easily accessible secondary literature on online platforms. Another factor in literature selection included content relevant to the research topic, such as blockchain application in the medical and healthcare sector and illustrating specific concerns and challenges [21]. The inclusion criteria for picking a specific article for the study are addressing medical data encryption and emphasizing the challenges and concerns relevant to the encryption process.

Researchers prioritized data collected via random procedures when selecting secondary literature to incorporate into the study [34]. An evaluation of scholarly article abstracts and titles occurred alongside an extensive analysis after generating a hard copy of the articles. Confirming the relevance of the articles about the topic of evaluation occurred by subsequently scanning the sources. The only articles accepted were those with content pertinent to the topic of medical data encryption concerns and challenges.

2.3 The process of data collection

The 'researcher's search evaluated the relevant documents to highlight the variations of medical data encryption and associated concerns and challenges. Appropriate scholarly sources encompassed periodicals, articles, and books focusing on content about medical data trust and encryption and concerns and challenges over time [37]. Generating relevant articles and books occurred using the university database. Specific keywords sufficed to generate the initial articles. The researcher performed a search for articles using various databases, such as PubMed, EBSCOhost, ERIC, and Google Scholar. The keywords used for the general search included medical, data, and encryption. Paper and article selection occurred relevant to the search results so long as the respective sources aligned with the relevant inclusion criteria.

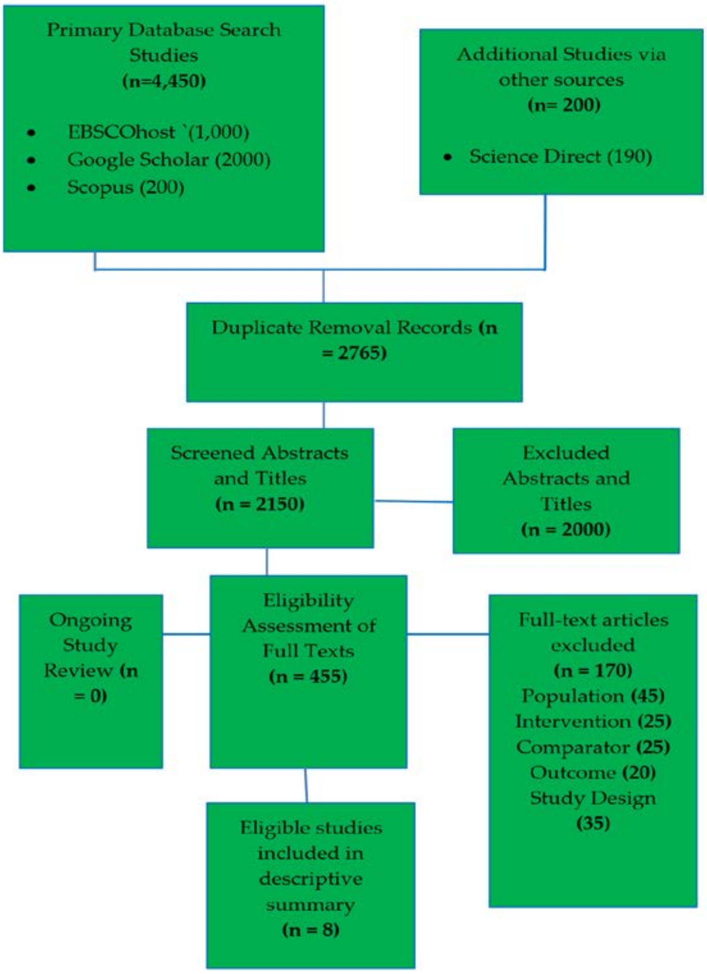
Primary Database Search Studies
(n=4,450)
EBSCOhost `(1,000)
Google Scholar (2000)
Scopus (200)
Additional Studies via other sources
(n= 200)
Science Direct (190)
Duplicate Removal Records (n = 2765)
Screened Abstracts and Titles
(n = 2150)
Excluded Abstracts and Titles
(n = 2000)
Ongoing Study Review (n = 0)
Eligibility Assessment of Full Texts
(n = 455)
Full-text articles excluded
(n = 170)
Population (45)
Intervention (25)
Comparator (25)
Outcome (20)
Study Design (35)
Eligible studies included in descriptive summary
(n = 8)

Figure 1. PRISMA flowchart Source: (Generated by the Authors)

A specific highlight of the search outcomes reveals that the search generated 4450 records, encompassing health organization records and conventional research studies. Regardless of the accessibility of a large amount of data because of the search strategy, the researcher removed all the duplicates using the process of data cleaning. After eliminating duplicate sources, the researcher remained with 2765 articles. In addition, a review of abstracts and titles occurred to confirm that the sources aligned with the relevant inclusion criteria. The final elimination occurred pertinent to the research designs and methodology. The PRISMA study flowchart, figure 1, demonstrates the search results.

2.4 Synthesis and analysis of data

Ongoing and recursive data analysis protocols were applicable for data analysis. The specific occurrences entailed reading literature review contents and grouping them pertinent to various themes [35]. The current study focuses on assessing the concerns and challenges of medical data encryption and suggests strategies for addressing such concerns and challenges [33].

2.5 Ethical consideration

Generating relevant approvals from specific authorities was the first step toward addressing the arising ethical concerns. In addition, the literature generated while carrying out the research occurred with a faithful intention, such as proper acknowledgment to eliminate plagiarism via reference listing.

3. Findings and discussions

3.1 Application of Blockchain within the healthcare system

Blockchain assists in maintaining and sharing the relevant medical records of the patient with the relevant group of healthcare providers and the hospital. Numerous specific applications include, including y of drugs and patient monitoring oER.

3.1.1 Drug Traceability

Traceability of drugs is always undertaken using a centralized approach within which aspects such as authentication and privacy of data, as well as the system flexibility, are never realized. Several decentralized models have always been proposed to solve issues related to drug traceability. For the privacy and authenticity of traceability data, a blockchain system known as Drugledge has widely been proposed. Drugledger usually integrates the Blockchain with the whole drug supply chain to easily trace such drugs [3]. Drugledger specifically has two different flows of drugs: the information that flows regarding the drug ledge and the physical flow of the real drug, all of which goes to the drug ledge network in the formula of a chain network of drugs. This new system alters the traditionally understood protocols by grouping the healthcare professionals into various parts: QSP, query service provider; CSP, certificate service provider; and ASP. However, it is important to note that the drug traceability scenario, as illustrated in the present paper, looks so simple theoretically but is very complex within the real-life case scenario.

However, Hamza et al. (2020) [3] highlight that the entire drug traceability system becomes more reliable and secure when the internet of things Bis is integrated with blockchain. Numerous frameworks have been suggested in the healthcare field regarding drug traceability or patient monitoring systems. The researchers in [4] suggested a structure to help curb drug fraud by tracking every drug within the supply chain system. The greatest aim in this scenario is to help reduce incidences of counterfeit drugs within the Blockchain. The specific and commonest technologies that can be applied to help improve the traceability and visibility of commonest technologies that can be applied to help improve the traceability and visibility of commodities such as drugs are RFID and Blockchain.

For a more transparent movement of the drugs, the Gcoin Blockchain model, in which G stands for the global control, is suggested; the model equally changes the drug supply chain system from regulating to inspection and surveillance of the drugs [6]. This means a government model that is combined with a decentralized autonomous organization.

Blockchain is applied to develop a kind of atmosphere where two different parties can trust one another. There are numerous ways through which Blockchain can be implemented, though the common approach, as claimed by Siyal et al. (2019) [4], is Gcoin Blockchain. As further argued by the scholar, Gcoin Blockchain can easily track every drug in the same ways Blockchain tracks the movement in bitcoin. It assists in building a high level of trust and transparency between sellers and buyers [4]. It is important to note further that Gcoin aims to improve overall data efficiency.

In India, for instance, several lives are considered at risk due to toat r. As a result of risk due to the use of fake drugs. A proposed framework of Blockchain can therefore be applied to help detect the possibility of fake drugs within the supply chain. Such suggested frameworks are based on

Hyperledger fabric kind of architecture, within which one PC works as the main beneficiary and five different computers are applied when making the orders. The system is fully dependent on blockchain technology [8]. Moreover, the supply chain of drugs from the drug-producing stores to the local intermediaries and clinics or retail drug shops and hospitals is managed by the application of Blockchain, which assists in tracking all the fake drugs.

The system, in this case, was tried in several case scenarios such as audits of drugs in distribution, stolen drugs, or fake distribution of drugs. The blockchain system was compared with other systems in numerous parameters such as resistance against any given point of failure, detection of counterfeit drugs, identification of diverted drugs, spying for drug shortage, security, privacy, transparency, and immutability [9]. However, Makridakis et al. (2019) [5] outline that the blockchain system never poses the capability of discovering and eliminating the usage of drugs that have not been authorized.

Regarding medicine, the commonest threat is that the manufactured medicine is never received by the pharmacy and can easily get replaced with a counterfeit supply chain. As emphasized by [11], the supply chain approach can never trace drugs that have landed on the wrong hand. For instance, India produced the majority of the counterfeit medicines in 2017 and presently approximated that close to 35% of counterfeit medicine were sold across different parts of the globe. To come out from these problems, Abunadi (2021) [12] proposed the usage of Blockchain and claimed that it is more transparent since one change in the transaction process will automatically get reflected by all the relevant users. With its Bdecentralization concept of decentralization, Blockchain can analyze the results on two different platforms: Hyperledger and Ethereum. Within Ethereum Blockchain, every operation needs some fees. Miner is provided money to perform transactions and maintain the Ethereum network [10]. There has never been a major need to know your Customer (KYC) within such a process, resulting in some sort of the blind spot which shows us the individual who might be using the account. Blockchain applying Hyperledge, on the other hand, never needs fees, making it easy for the individual producer to undertake the transaction.

3.1.2 Electronic Health Record

An electronic record includes the necessary vital administrative and clinical data of the patient like demographics, diagnosed clinical problems, medication, and laboratory data, among other reports. Using paper as a means of recording patient data has proved to be very extensive and non-reliable as the world has since gone digital [11]. As a result, most healthcare organizations have resorted to using electronic records to keep their data. Blockchain, a decentralized type of database whose data block is specifically linked chronologically, has widely been applied to enhance HER performance. Arunkumar (2020) points out that rivatenumerous parties within the healthcare industry need to manage the personal HER blockchain collaboratively, like the medical specialists, insurance departments, and the hospital. Since the traditionally known EHR system is trademarked with decentralized design, only one unit of supplier controls the code base, database, and system outputs. It has become difficult for the centralized systems to have full confidence from the hospital management, doctors, and patients [12]. Therefore, Blockchain has been considered the solution to the trust issue associated with a centralized electronic health record system. With blockchain technology, all the patient information is stored in the Blockchain through the use of meta ma,s, and the details of each patient are stored in the blockchain as independent data blocks. Each block comprises encrypted data. The system record health-related information of an individual patient so that it can easily be consulted by respective health care providers and the patients themselves. In most cases, the data is usually encrypted by a specified algorithm to encrypt all the patients' data into a single line bit that is subsequently stored in the block [5].

As Donawa et al. (2019) noted, using blockchain in electronic health records offers a convenient health record storage service that promotes easy accessibility of such records through the web. The system is often designed to allow the patients full control of generating, managing, and consequently sharing their electronic health records with friends, family, healthcare providers, and other relevant data consumers. Abunadi (2021) [12] illustrates that such a system's main advantage is security and confidentiality. Scholars acknowledge that a blockchain system is more reliable and secure than paper storage of medical records. However, it is important to note that several issues of concern are still linked to the usage of blockchain in electronic health records. Present paper aim present paper present paper aims to offer a detailed analysis of the issues and concerns regarding the usage of blockchains in electronic health records. For instance, Alla et al. (2018) [19] point out that the patient may lose control over the existing healthcare data during live events, even though the service provider always maintains the primary stewardship. Patient access to their information might be very much limited, and they might be typically unable to share such data with ease with the relevant providers or researchers.

Cunningham et al. (2018) [25] report that Blockchain has always been proposed to address the issues attributed to data access and privacy. Fatokun et al. (2021) [28] explain that it is a blockchain for electronic health records, that is to say, a growing list of blocks comprising records linked through the application of cryptographic hash. There are numerous advantages linked to blockchain in electronic health records. For instance, a Blockchain is a linked peer-to-peer database in which data integrity, availability, and response time are fully guaranteed. Blockchains can adequately facilitate internet of things security in electronic health.

Moreover, the Blockchain works within the governance model, which helps enforce business logic that all the participants accept. It is, therefore, very possible to exploit a smart contract or chaincode to control the relevant control policy on access and achieve HIPAA compliance. Keshta et al. (2021) [29] also highlighted that Blockchain is additionally managed collectively by the relevant stakeholders, some of whom. Some have the right to record data in the block that cannot alter retroactively.

Mehta et al. (2020) [24] noted that blockchain in the electronic health record is distributed and append access rights to only its ledger shared among the specified users. Fine-grained access to the ledger is equally implemented to realize an appropriate balance between availability and privacy. Figure 2 below illustrates the possible access rights of users as applied in the BlockHealthChain. The rights, in this case, include read permission, write permission, read permission with anonymized EHRs, and authorization permission.

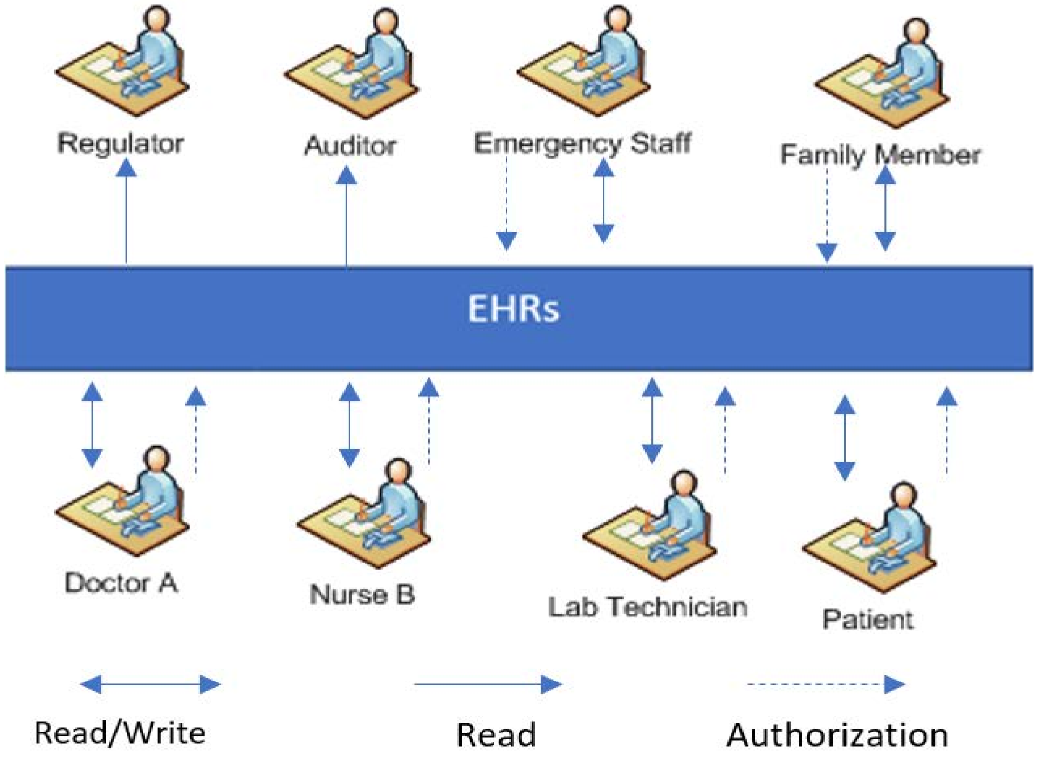

Figure 2. Possible access rights of users as applied in the BlockHealthChain.

It is clear from the figure that within blockchain protocol, different users tend to have different access qualifications for EHRs. With this arrangement, patients have the right to control access to electronic health records, including the individual patient-reported information. The former comprises numerous contents like allergies, demographic information, and numerous contents allergies, demographic information, and monitoring data collected from the applied instruments. The latter, in this case, refers to the updated medical record by the staff of doctors. The patient can authorize family members or health care providers to read and write their personal health information, minimizing the potential risks of tracking and replicating healthcare data.

Nurses, doctors, emergency staff, and laboratory technicians control and manage access to the electronic health record that is updated by themselves. Additionally, they make good use of or disclose protected health information for the diagnosis, treatment, and payment without seeking authorization from the patient [15]. This means having the authorization to grant read or write permission to other relevant entities, in which case the electronic health records are shared within the healthcare organizations.

Attaran (2020) [23] further points out that various groups of users submit numerous electronic health records. These may include test results, encounter notes, and demographic. For instance, the test result includes several fields: Patient ID, patient name, technician ID, type, indicator, and final result. Each electronic health record in the blockchain corresponds to a transaction, which must be executed accurately and included within the ledge. All the electronic health records pose lifecycle as shown in figure 3 below.

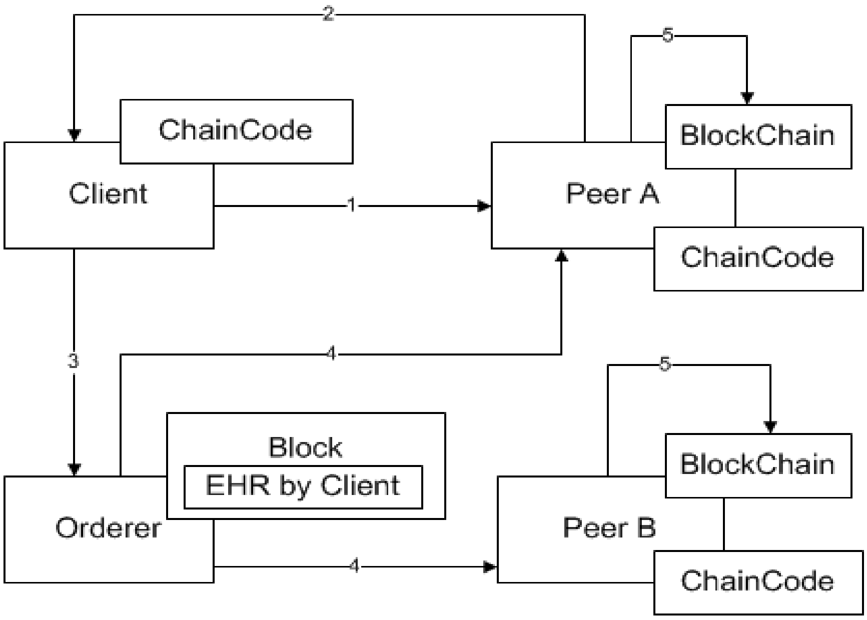

Figure 3. illustrates the electronic health records lifecycle

3.2 Challenges and issues associated with using Blockchain in the healthcare sector

The major challenge in the application of blockchain technology within the healthcare sector includes interoperability, security, Lack of Standardization, storage requirements, hesitant of hospitals to share the patient' ' data, lack of trust among patients, Lack of Skills among Doctors and Medical Practitioners, and lastly, accountability and data ownership.

Interoperability within healthcare means exchanging relevant information with each other within the entire blockchain network. It is the major concern based on the large and diverse group of providers and its large open existence [16]. There might exist various players such as private doctors, physicians, insurance institutions, players such as private doctors, physicians, insurance institutions, and players such as private doctors, physicians, insurance institutions, and hospitals, among others. Ensuring appropriate interoperability among different institutions may be a great challenge in healthcare.

Moreover, the idea of decentralization is considered very much secure, and some other security issues are associated with it. Since data are usually decentralized within the Blockchain, meaning such personal data are widely distributed within the public ledger, this can result in privacy leakage. Blockchain offers an environment where people trust or know and can securely share data. In some case scenarios, however, such objectives may fail, especially when those who have access to such data become malicious in their dealings [17]. A majority of the patients may become highly uncomfortable in making public or sharing their individual medical information as a result of security reasons.

Nagasubramanian (2020) also points out the handling, storage requirement, and scalability issue [15]. It is not practical to safely maintain data for all the patients. The medical record is usually in the form of laboratory reports, images, and documents. Storage of medical records of various groups of patients using digital methods may need colossal storage capacity [16]. The medical transaction of every individual stored in a distributed way with the same type of record stored in different locations may need some huge extra storage capacity, which may significantly impact the healthcare system.

Blockchain does not have adequate Standardization, even though it is a trending technology adopted worldwide. Within networks and domains where the concepts of trackability, trust, and security are involved, Blockchain seems to be lacking the most appropriate standardization. Attaran (2020) [23] reported that proper standardization of technologies and protocols is essential. Aspects such as data size and format may be sent to blockchain Blockchain, and whatever can be stored within the blockchain has to be defined clearly.

Equally, the hospitals and the associated entities may be hesitant to share the specified information. Most hospitals may be reluctant to share their patient medical records and the associated data, for instance, in for-profit circumstances, as they would wish to charge different fees from their respective customers [18][27]. On a similar note, insurance institutions and hospitals might be reluctant to share their data, as it might be advantageous for the healthcare institution to keep the fees-related data among themselves. It is very important to build a strong trust between the concerned parties and convince them to share their data for appropriate healthcare service delivery.

Lack of trust among the patients and other important stakeholders is also a major issue in applying Blockchain within the healthcare system. As argued by Attaran (2020), building trust among patients and other relevant stakeholders is essential for the success of any technology-driven healthcare and medical system [23]. Most patients might be reluctant to disclose and share their medical records within the public domain with other entities in the third party. Therefore, it is very much required to build confidence and trust among the individual patients regarding the privacy and security aspects of Blockchain in the healthcare system [12].

Additionally, asking physicians and other groups of healthcare providers to move from paper to technology can be a major challenge. Electronic records and prescriptions rather than paper-based prescriptions can be a major challenge to most people. For example, doctors always do not fill the fields considered to be unnecessary within their routine work. Despite all that, in the case scenario of electronic records, the physicians cannot omit the fields that have been marked as mandatory. On a similar note, depending on technologies such as Blockchain and the Internet of Things for remote monitoring can generate questions among physicians concerning their efficiency and accuracy [7]. Technology-related healthcare accuracy, performance, and efficiency depend on the doctor's skills and training. Therefore, before introducing such technologies into the actual practice, adequate training and the necessary skills should be imparted to the respective doctors to help build their confidence in applying such technologies [26].

Attaran (2020) illustrates that data accountability and ownership are other major challenges in deploying blockchain technologies within the healthcare industry [23]. Banu (2020) reports that although cloud sharing usually makes it easy and convenient to transfer the medical image, subsequently improving and streamlining the overall patient care, the major stumbling block to its widespread usage is still fear and unease regarding the technology. There are several issues and concerns regarding storing and sharing relevant medical images. Possibly the main hurdle for numerous practices and facilities is the right high-speed bandwidth required to transfer images quickly. Primary deduplication, storage, and compression will help dramatically minimize bandwidth usage while improving performance. Due to low bandwidth, image latency has become essential for the relevance of the cloud’s relevant user communication of the image by the users, and relevant performance criteria usually drive analysis applications. It is unclear that remote rendering offers low display latency for all the relevant medical imaging applications when assessing the server via the internet is necessary.

Ethics is the main guide of the moral consciousness among health care professionals. Confidentiality (also called Secretiveness) is one of the core principles of ethics. The relationship between the patient and the medical expert is only based on trust [30]. Therefore, every image data needs to be made under the main premise that all health information of any given patient will at all times be made confidential not only by the healthcare provider but also by any other individual with the legal and professional right to access such records. There is always a great need for such information to be protected from access by any unauthorized persons or disclosure to any family member except in the circumstances that it is required by law or in the situation where the patient has given out consent in writing [6]. The above findings show that most healthcare organizations still use paper record sets. Healthcare organizations still use paper records for each patient. Few medical practitioners have been reported using normal computer software for data encryption. This is contrary to other 'scholars' arguments that medical image records must always be stored in a safe place without failure to attend to. The universally accepted standard for keeping such data requires that if an electronic system is applied while entering the image of the patient, then there is a need for it to have a password and login for anyone to access such image [7]. There is also a great need to perform m backup of all the records on the removable medium that will enable the recovery of data images in the event the system fails. A breach of confidentiality is always considered to have occurred when the private information that a given healthcare provider has learned from the patient is passed to the third party without permission from the patient or court order.

Literature has affirmed that Information communication in the current times has become more effective and efficient. However, security concerns over safe data transfer have been rising [31][36]. Cyber-attacks and other related threats targeted at the system of information communication render network and system security an aspect worth considering deeper within the realm of information communication technology [15]. With the advance in technology, hackers and intruders have very complicated tools they can use to bypass the traditionally known generic network security system to cause intentional harm to the whole system. Specifically, cyber security threats are currently exploiting the connectivity and complexity found in the existing infrastructure and launches attacks on systems considered legitimate. Even with such predicaments, it is important to note that the performance of the healthcare industry depends on the reliable working of the important infrastructure, whose safety might be put at a higher risk by the cyber-attacks [11]. Such attacks have attacks has attacks have major impacts on the general viability of the healthcare organization that might have been affected and even on the general company reputation. System failures and crashes are good examples of the risks that most organizations currently dread in their daily operations. For this reason, numerous security measures have been considered necessary even as blockchain technology is being implemented.

Among such measures has always been the detection system for any network intrusion. This system is taken to help secure the computing resources from malicious intrusion and attack threats [19]. Network Intrusion Detection System usually analyzes and predicts behaviors of a given system with the main aim of countering such activities that it might interpret as suspicious. The intrusion, in this case, can always occur in various ways: a legitimate user of a given system misusing the privileges they have of accessing the system, a legitimate user trying to gain additional access privileges, and an external attacker trying to access the system [20]. In this case, the network intrusion detection system works by either recognizing the attacks or malicious activities or blocking them or detecting them by looking at the signatures of the attack within the log files. However, organizations are yet to achieve much with the current network security systems; organizations are yet to achieve much with the current network security systems, even such a system.

Literature affirms that the ever' as well as uncertainty related to today's-increasing complexity and uncertainty related to the increasing complexity and uncertainty related to today's clinical decision situations necessitates healthcare providers to apply the most sophisticated quantitative models that move beyond the general capabilities of the known traditional simple linear models. As the uncertainty and complexity of the data continue to increase, the model's general capability need also needs to equally increase so that the highly nonlinear relationships within the existing variables can also be captured [14]. This is where artificial neural networks and blockchain technologies fit into clinical decision-making.

Such models can be traditional of various types: decision analysis, optimization, simulation, and other things. Artificial neural networks and blockchain applications represent the modern approach to modeling. Artificial neural networks and blockchain applications can also be associated with data-driven clinical decision support. In that regard, neural networks offer a method for analyzing or forecasting past data [9]. Though it is -commonly known as the black-box approach, or rather, a heuristic method, within the last decade, blockchain technologies have greatly been studied by the known statisticians to gain an accurate understanding of the individual power prediction from the statistical point of view.

4. Conclusion and Recommendations

The study has established numerous blockchain applications, including numerous specific applications, including traceability of drug and patient monitoring or Electronic Health Records (ERH). While Blockchain assists in maintaining and sharing the patient’s relevant medical records with the relevant group of healthcare providers and the hospital, it is important to note that ethics is the main guide of the moral consciousness among the health care professionals. Confidentiality (also called Secretiveness) is one of the core principles of ethics. The relationship between the patient and the healthcare professional expert is only based on trust. Every medical record is therefore needed to be made under the main premise that all health information of any given patient will at all times be made confidential not only by the doctor but also by any other members of the healthcare team who have the legal and professional right to access such records. There is always a great need for such information to be protected from access by any unauthorized persons or disclosure to any family member except in the circumstances that it is required by law or in the situation where the patient has given out consent in writing. As to protect the data from any project the data securely; the data from any above findings show securely, blockchain technology has failed to securely protect the data from unauthorized dealers. This is contrary to the academic expectations that always medical records must be stored in a safe place without failure to attend to. The universally accepted standard for keeping medical records requires that the theanectronic system is applied while entering the patient's records. It needs a password and login for anyone to access the data. This factor is not applicable in blockchain Blockchain as each data set is presented in blocks and can be accessed individually. There is also a great need to perform a backup of all the records on the removable medium that will enable data recovery if the system fails. A breach of confidentiality is always considered to have occurred when the private information that a given dental practitioner has learned from the patient is passed to the third party without permission from the patient or court order. Equally, Blockchain does not have adequate Standardization, although it is a trending technology adopted in numerous countries worldwide. Within networks and domains where the concepts of trackability, trust, and security are involved, Blockchain seems to be lacking the most appropriate Standardization. While those not concerned with the 'patient's data might intentionally attempt to access information on the 'patient's identity or location by intercepting communication between the patient and the healthcare providers, such efforts may be thwarted when proper security control systems are put in place. Numerous breaches can easily be prevented by putting a high-quality security plan specializing in the simplest and most common reasons for data breaches within the blockchain system.

Acknowledgment

The authors sincerely acknowledge the Princess Sumaya University for Technology and the Researchers Supporting Program (TUMA-Project-2021-14), AlMaarefa University, Riyadh, Saudi Arabia, for supporting steps of this work.

References

1. Regueegu FA, Mohd S, Hakami Z, Reegu KK, Alam S. Towards trustworthiness of electronic health record system using Blockchain. Annals of the Romanian Society for Cell Biology. 2021 May 20;25(6):2425-34.
2. Ratta P, Kaur A, Sharma S, Shabaz M, Dhiman G. Application of Blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality. 2021 May 25;2021.
3. Hamza S. U, Aslam S, Arjomand N. Blockchain in healthcare and medicine: A contemporary research of applications, challenges, and future perspectives. arXiv preprint arXiv:2004.06795. 2020 Mar 30.
4. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applying blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography. 2019 Mar;3(1):3.
5. Makridakis S, Christodoulou K. Blockchain: Current challenges and prospects/applications. Future Internet. 2019 Dec;11(12):258.

6. Dutta P, Choi TM, Somani S, Butala R. Blockchain technology in supply chain operations: Applications, challenges, and research opportunities. Transportation research part e: Logistics and transportation review. 2020 Oct 1;142:102067.
7. Goyal S, Sharma N, Bhushan B, Shankar A, Sagayam M. IoT enabled technology in secured healthcare: applications, challenges, and future directions. Cognitive internet of medical things for smart healthcare 2021 (pp. 25-48). Springer, Cham.
8. Khan SN, Loukil F, Ghedira-Guegan C, Benkhelifa E, Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications. 2021 Sep;14(5):2901-25.
9. Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. IEEE Access. 2019 Oct 9;7:147782-95.
10. Mayer AH, da Costa CA, Righi RD. Electronic health records in a Blockchain: A systematic review. Health informatics journal. 2020 Jun;26(2):1273-88.
11. Donawa A, Orukari I, Baker CE. I am scaling blockchains to support electronic health records for hospital systems. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) 2019 Oct 10 (pp. 0550-0556). IEEE.
12. Abunadi I, Kumar RL. BSF-EHR: blockchain security framework for electronic health records of patients. Sensors. 2021 Jan;21(8):2865.
13. Al-Haija, Q.A.; Alsulami, A.A. High Performance Classification Model to Identify Ransomware Payments for Heterogeneous Bitcoin Networks. Electronics 2021, 10, 2113. https://doi.org/10.3390/electronics10172113.
14. Alam S, Reegu FA, Daud SM, Shuaib M. Blockchain-based Electronic Health Record System for efficient Covid-19 Pandemic Management.
15. Nagasubramanian G, Sakthivel RK, Patan R, Gandomi AH, Sankayya M, Balusamy B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications. 2020 Feb;32(3):639-47.
16. Reegu FA, Al-Khateeb MO, Zogaan WA, Al-Mousa MR, Alam S, Al-Shourbaji I. Blockchain-based framework for interoperable electronic health record. Annals of the Romanian Society for Cell Biology. 2021 Mar 30:6486-95.
17. Yao Y, Kshirsagar M, Vaidya G, Ducrée J, Ryan C. Convergence of Blockchain, autonomous agents, and knowledge graph to share electronic health records. Frontiers in Blockchain. 2021 Apr 6;4:13.
18. 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.
19. Alla S, Soltanisehat L, Tatar U, Keskin O. Blockchain technology in electronic healthcare systems. InIIE Annual Conference. Proceedings 2018 (pp. 901-906). Institute of Industrial and Systems Engineers (IISE).
20. Chelladurai U, Pandian S. A novel blockchain-based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing. 2022 Jan;13(1):693-703.
21. Q.A. Al-Haija, M.Alnabhan, I.Saleh, M. Al-Omari 'Applications of Blockchain Technology for Improving Security in Internet of Things (IoT)', Book title: Fostering security in IoT Healthcare using Blockchain Technology, To appear in "Cognitive Data Science in Sustainable Computing " series, Elsevier. 2022. (In Press)
22. K. Albulayhi, Q.A. Al-Haija, Chapter: Security and Privacy Challenges in Blockchain Application, Book Title: The Data-Driven Blockchain Ecosystem: Fundamentals, Applications, and Emerging Technologies" ISBN: 978-1-032-21624, To Appear, CRC Press (Taylor & Francis Group). 2022. (In Press).
23. Attaran M. Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management. 2020 Nov 7:1-4.
24. Mehta S, Grant K, Ackery A. Future of Blockchain in healthcare: the potential to improve the accessibility, security, and interoperability of electronic health records. BMJ Health & Care Informatics. 2020;27(3).
25. Cunningham J, Ainsworth J. Enabling patient control of personal electronic health records through distributed ledger technology. Stud Health Technol Inform. 2018 Jan 31;245:45-8.
26. Ramachandran, S., Kiruthika, O.O., Ramasamy, A., Vanaja, R., and Mukherjee, S., 2020, September. A review on blockchain-based strategies for management of electronic health records (EHRs). 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 341-346). IEEE.
27. Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare ": "MedRec" prototype for electronic health records and medical research data. InProceedings of IEEE open & big data conference 2016 Aug 13 (Vol. 13, p. 13).
28. Fatokun T, Nag A, Sharma S. Towards a blockchain-assisted patient-owned electronic health records system. Electronics. 2021 Jan;10(5):580.
29. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021 Jul 1;22(2):177-83.

30. Tang F, Ma S, Xiang Y, Lin C. An efficient authentication scheme for blockchain-based electronic health records. IEEE Access. 2019 Mar 13;7:41678-89.
31. da Conceição AF, da Silva FS, Rocha V, Locoro A, Barguil JM. Eletronic health records using blockchain technology. arXiv preprint arXiv:1804.10078. 2018 Apr 26.
32. Torres-Carrión PV, González-González CS, Aciar S, Rodríguez-Morales G. Methodology for systematic literature review applied to engineering and education. In2018 IEEE Global engineering education conference (EDUCON) 2018 Apr 17 (pp. 1364-1373). IEEE.
33. Tranfield D, Denyer D, Smart P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British journal of management. 2003 Sep;14(3):207-22.
34. Ferreras-Fernández T, Martín-Rodero H, García-Peñalvo FJ, Merlo-Vega JA. The systematic review of literature in LIS: An approach. InProceedings of the Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality 2016 Nov 2 (pp. 291-296).
35. Crowther M, Lim W, Crowther MA. Systematic review and meta-analysis methodology. Blood, The Journal of the American Society of Hematology. 2010 Oct 28;116(17):3140-6.
36. de FSM Russo R, Camanho R. Criteria in AHP: a systematic review of the literature. Procedia Computer Science. 2015 Jan 1;55:1123-32.
37. Rother ET. Systematic literature review X narrative review. Acta paulista de enfermagem. 2007;20:v-i.