Research Article

Patient's Complete Control of Electronic Health Record (EHR) Using Blockchain Method

ABDULAZIZ M ALZAHRANI & Prof:MUHAMMAD S. RAMZAN[1]

[1]*Department of Information System, King Abdulaziz University, Jeddah, Saudi Arabia*

Correspondence should be addressed to Abdulaziz M Alzahrani; aalzahrani3529@stu.kau.edu.sa

Academic Editor:

Abstract

Patients can store their health data in their electronic files and grant permission to physicians around the world to view the data and possibly amend it if needed. This increases data integrity risks, which can be compromised or exploited for various purposes. The researchers are keen to find methodologies by which data can be safely transferred and stored.

This research proposal will use blockchain technology to protect patient-sensitive electronic health records (EHR) without exposing their data to the risk of being violated or adding unwanted details. The patient will register on Blockchain for creating their electronic health record and share their medical report with the doctor to diagnose the health condition. The patient will check the medical report and either accept it as a new block in their electronic health record in the Blockchain or reject it. The patient's identity will be hidden in the Blockchain (as is the case with Bitcoin users). The prototype model will be implemented using the MATLAB tool.

Keywords: Electronic Health Record (EHR), Blockchain Technology, Identity Hiding, Integrity and Confidentiality, Medical Authorities

1. Introduction

Modern technology has become an essential tool for doctors as it is used to follow up patients infected with a pandemic disease like Coronavirus, which is spreading rapidly around the world during the year 2020 (Singh, 2020). Electronic health care has become an essential requirement for the overall growth of urban countries. This led to the transition from the traditional approach that relies on long-established documents to a modern style based on electronic storage. Storing health data has become faster with less effort and cost, which is a significant development. Electronic Health Records (EHRs) technology is helping many doctors through continuous communication and health follow-up of patient cases such as blood pressure, heart rate, and diabetics. Also, the patient can store his health data in particular files and permit various stakeholders such as doctors and agencies located worldwide to see the data and some time to edit if needed. However, this means medical data is exposed to the Internet, which opens the desire of cybercriminals to exploit that. There is a need to find a secure method to protect the electronic health records (EHRs), which are hacked and breached by cybercriminals, despite the presence of multiple methods available that prove security limitations. There are several ways to hack patients' electronic records, such as a health facility's web penetration or an SQL compromise database at a data storage center or the host's site. For example, there is a test on different methods of protecting patient data, and the most common penetrating method is related to accessing patients' accounts on a system called Egton Medical Information Systems (EMIS) EHR (MacKenna, 2020). Another article confirms (Verizon, 2019) officially, over 2000 data records were hacked during 2019.

On the other hand, the health-related staff is not well trained about the sensitivity of health data and does not have knowledge about cybersecurity and the risk of penetration (Kamerer, 2020). All these emphasize the need to use a powerful method to protect critical EHRs. Blockchain technology in health care has achieved great success (Sharma, 2020) in different ways. The feature of decentralized administration is the essential thing that will give Blockchain the power to revolutionize healthcare. The approach of decentralized administration makes every patient control information and exchange it when needed. The health care sector also deals with fast and easy access to confidential information. Therefore, Blockchain technology can assure the secure transmission and sharing of that information completely safe. The Blockchain also ensures the privacy of information and the confidentiality of access regardless of the limitation of numbers of users. The conceptual model of the use of Blockchain will be demonstrated with multiple scenarios to secure and protect the EHRs. We will test the proposed model using a scientific tool like MATLAB. The model consists of the following steps to ensure proper security and secrecy:

1. The patient registers and creates an account on Blockchain for his/her electronic health record.
2. He sends the request to diagnose his health condition to the doctor.

3. Then the doctor records his medical report and sends it to the patient in a simple way to understand it.
4. The patient will check the medical report and either accept or reject it.
5. If the patient accepts the medical report, the report will be added as a new block in his/her electronic health record in the Blockchain.
6. The patient's identity is hidden in the Blockchain (as is the case with Bitcoin users). The patient's data appears without the visibility of his/her identity, and it is a helpful feature from a security point of view, and only relevant authorities can access that medical record.

Sometimes, the doctor hides the type of disease from the patient as (Wang, 2019) believe that the patient does not need to view his electronic health record in consideration of his psychological conditions. For example, if a person is diagnosed with cancer, the patient's family is notified. In fact, it is contrary to medical diagnoses that say, as stated by the author (Simonton, 1992), knowing the patient's type of illness with its details helps the patient participate in the speed of his body's response to treatment and healing. The research also suggests the necessity of relying on health centers and hospitals by establishing nodes within each large health facility instead of relying on external parties such as Oracle or Ethereum. The researchers noted that there are downsides to relying on these external parties, including:

1- Relying on the central Oracle as an intermediary to access the decentralized Blockchain eliminates the advantage of smart contracts and makes them like regular contracts, which increases security risks. Researchers (Caldarelli et al., 2021) have indicated decentralization risks if intermediaries such as Oracle are involved.

2. The supply remains under the control of Oracle, which brings us back to the principle of centralization that is incompatible with the principle of Blockchain, even if Oracle controls multiple nodes.

3- Oracle only relies on Ethereum for smart contracts that also rely on gas for storage (Wackerow, 2021); Ethereum-related issues such as gas price hikes may affect Oracle. We can follow the prices for the last month through (Ethgasstation, 2021), which shows us the high cost of each operation.

2. Brief Review of (EHR) Using Blockchain Method

Blockchain technology helps eHealth systems to provide patients and medical institutions an effective and flexible option to manage their EHRs. IBM cooperated with the Blockchain Institute for Research and proposed establishing more privileges in the use of blockchain technology by laying the foundations for patient monitoring. It also suggested that the patient be allowed to share his data with a third party for personal or humanitarian goals of research centers, and no one has been accomplished (Wiljer, 2019). In the article (Vora J. I.-1., 2018), they believe that providing high privacy to patient data has become complex with the development of health care and its association with technology. These proposals from IBM and the Blockchain Research Institute urge the researchers to find more accurate solutions. Recently, several authors have proposed using blockchain technology approaches to treat the problems that face the safety and security of electronic health records (Shamshad, 2020) (Adlam, 2020) (Shi, 2020). (Liang, 2017) proposed a technique for data sharing and collaboration in mobile health applications. He described a method in a mobile application that is conveyed to gather health information from individual wearable devices, manual input information, therapeutic devices, and information synchronization to the cloud to impart information to social insurance suppliers and health care coverage organizations. The system of that application contents of six entities. The first entity is the patient, the owner of personal health information,

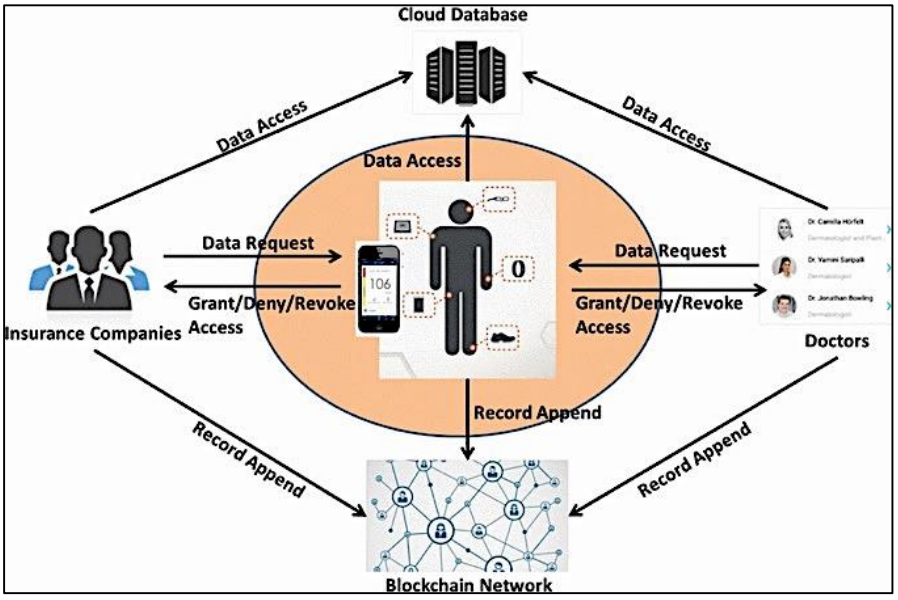

Figure 1: The model system design (Liang et al., 2017)

and is liable for allowing, denying, and renouncing information access from other companies. Second is the wearable devices, which transform original health information into readable information and then synchronize it to their online account. The third entity is healthcare providers such as doctors who have been pointed indeed by

the user to perform the medical tests. The fourth one is the insurance company. The fifth is the cloud database for storing data, and the last entity is the blockchain network (Figure 1).

This article is a good initiative by securing the patient data have a secure record and secure processing. However, the model has a limitation of recording data that each request or update from the healthcare insurance suppliers or the medical coverage organizations is recorded and moored to the blockchain network, which makes the action on the patient's data crucial and sensitive.

The article (Chen et al., 2019) suggested using blockchain technology to search and share electronic health records. The author recommended that while most of the patients' information is rarely changed, it is better to use Blockchain to activate this feature safely. Moreover, the author thought that while the patient information is researchable from any hospital or dental center that the patient wants to share, it is better to use this technology with a high confidence level. Finally, the paper suggested actualizing a proof-of-concept study in future research to evaluate its performance in a real-world environment. The author discussed security issues in cloud computing for the electronic health record (EHR). This article is a good initiative by contributing the client's figuring ability to include a new block to the Blockchain, and he earns a reward from the final work when he shares his data with one of the beneficiaries, which is a motivating idea for data holders. The authors proposed storing the entire health records in a centralized public cloud server. The model also has a limitation of testing on a single computer with an Intel Core i5 and 2.5 GHz processor with a memory of 8 GB, coding typed in Python 2.7 and MongoDB. Moreover, there is no available EHR database; they used the Nursery database from the University of California (Chen, 2019).

The article (Cao, 2019) clarified how eHealth systems are secure from tampering EHRs via Blockchain using TP-EHR. The TP-EHR is mainly constructed on the security of the Ethereum blockchain. Moreover, even if the doctor does not have ethics, the EHR is secure and impossible to edit, especially when using TP-EHR. The authors recommend activating this technique to achieve the features. One of these advantages is accessing their specific doctor and making appointments with him. Also, TP-EHR performance can be evaluated in terms of connection and general expenses. When writing this article, the transaction in Ethereum costs approximately 8 US cents, which is an affordable cost. This paper proposed utilizing TP-EHRs to secure data on cloud computing depending on the security of Ethereum. The author made proof of TP-EHRs through the adversary model. I think this paper is so far good in practice. On the other hand, the author believes that the security test has proved TP-EHR secure instead of different attacks happening in the current cloud-support of eHealth program, but what if the doctor's computer was hacked, what should be the solution?

The proposed technique (Tanwar, 2020) has suggested an EHRS application based on blockchain technology to address the limitations of the healthcare scheme. The paper suggests a control policy algorithm for increasing data accessibility between healthcare institutes, helping to simulate the environments to execute the electronic healthcare record (EHR) distribution scheme that utilizes the idea of a chain code. The article proposed an excellent algorithm for protecting patient data from being compromised or modified. However, the authors argue that the scheme of the (EHR) distribution should be decentralized in controlling and relying on establishing a blockchain network in more than one location. This limit reduces the spread and expansion of this technology, and this scheme becomes more expensive than other alternative methods.

The article (Tripathi, 2019) put forward the S2HS-A (Secured and Smart Healthcare System) approach for an intelligent healthcare system based on Blockchain. The article examines the technological, social, and cultural barriers to accepting blockchain technology by analyzing and evaluating developers and experts in the field while visualizing the end user's needs. It is proposed to design a framework for the intelligent healthcare systems (SHS) approach by utilizing various sensor types with different functions and techniques used to provide the required security and system integrity. Moreover, the system S2HS has overcome the issues faced by SHS. That system has five prime entities (IoT-based Wearable Devices, Electronic Health Records/Clinical Data, Encryption/Decryption and Standardization, Blockchain Mechanism, and End Users) as shown in figure 2. The dimensions of future research and the possibility of using blockchain technology in health fields were also discussed. This paper added a reasonable proposal on the SHS suggestion with the Consensus Protocol Technique, which makes human error rare, unlike traditional databases. The reason is that data entry in the Blockchain is unanimous. However, there are limitations, such as not applying the model to actual samples to measure its success rate. Implementing this approach also requires internationally recognized standards to be adopted easily. Health care organizations and patients should accept the use of the suggested sensors.

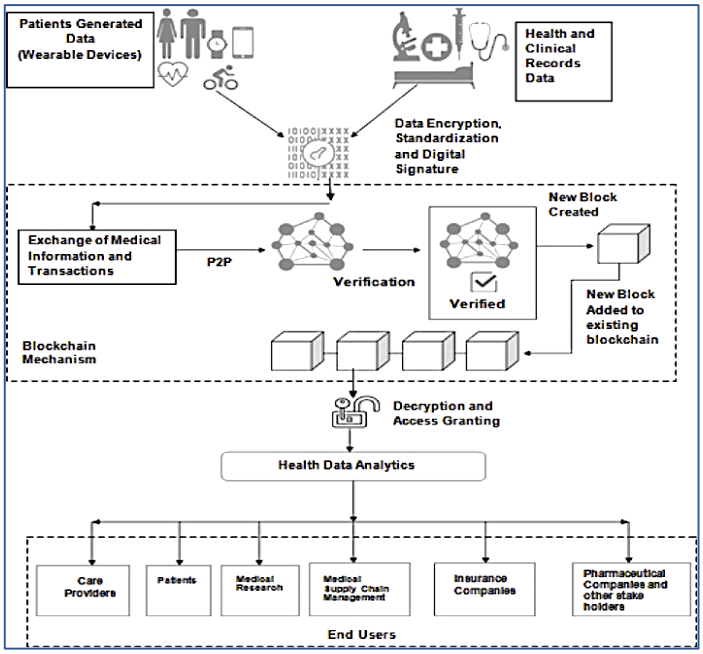

Figure 2: The system S2HS entities (Tripathi et al., 2019)

The article (Nguyen, 2019) suggested that there should be an approach using new tools with Blockchain. This approach has EHR Manager connected with the user's mobile, admin, smart contracts, decentralized storage, and data block structure, as shown in figure 3. Having a central EHRs Manager was not a good approach, especially

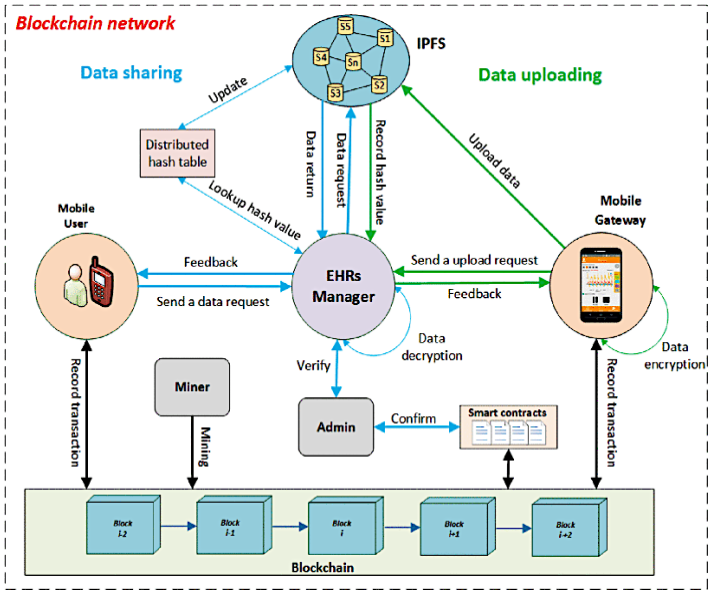

Figure 3: The proposed data flow of smartphone with the blockchain system (Nguyen, 2019)

since this manager was responsible for encrypting and decrypting patient data. It thus becomes a target for hackers and malicious people.

The article (Sharaf, 2019) suggested the government framework for the health records system based on the multi-authority encryption policy and sharing the encryption keys for electronic health records with confidence

to a central trusted health authority (THA). However, this proposal relies on creating a party with governmental authority and operates as a central data store, but if that authority is compromised, then all the encryption and decryption keys for the EHR stored in it will be hacked.

(Y. Zhuang, 2020) suggest using smart contracts (Ethereum) in the communication processes between patients, doctors, and health facilities. Still, on the other hand, he suggests creating a node using a mobile phone or an ordinary computer, and this contradicts the specifications of the approved node devices on the Ethereum website (ethereum.org, 2021). The authors further suggested creating an external database in every clinic to store all the patient's data that was added locally, which violates the principle of the Blockchain, which is not to keep the data in a specific place. Maybe his suggestion was to ease the slow data transmission and connection to the Blockchain. We suggest storing data on the Blockchain for two main reasons to solve this problem. First, to protect patient data from the possibility of penetration of local databases, all data and reports are registered with a traditional technique. Second, the time is taken, which occurs due to waiting for the receiver to obtain approval from all nodes that their data is accurate and correct. Therefore, to avoid a waste of waiting time, this research suggests a process to verify the validity of the new block data through the connected nodes with a percentage of 100% if the number of nodes does not exceed 500 nodes.

Still, suppose it increases to be more than that. In that case, the data validity is verified through the random selection process. This number does not exceed the total number of nodes worldwide, which this research proposes to treat.

(Madine, 2020) suggests relying on Oracle to manage health records using smart contracts powered by blockchain technology (Fig4).

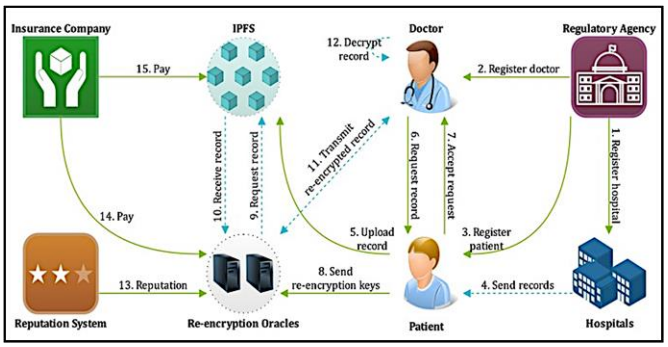

Figure 4: Main Components of the System

Oracle is considered a reputable company, but the proposal to rely on a centralized Oracle as an intermediary to access the decentralized Blockchain as (Fig5) eliminates the advantage of smart contracts on the one hand and makes them like regular contracts, which increases security risks. The researchers *(Caldarelli, 2021)* indicated

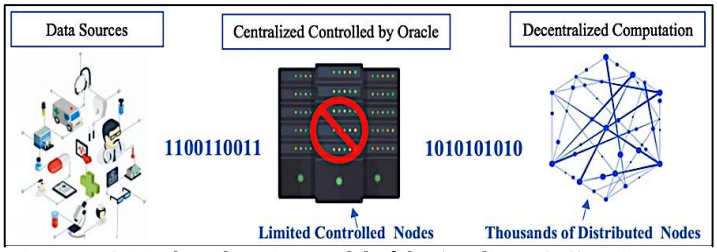

Figure 5: Critical Explanation Model of the (Madine, 2020) main components system

decentralization risks if intermediaries such as Oracle are involved, especially in retrieving external data. On the other hand, the supply remains under the control of Oracle, which brings us back to the principle of centralization that contradicts the focus of the Blockchain, even if Oracle controls multiple nodes. Moreover, Oracle only relies on Ethereum for smart contracts and gas for storage *(Wackerow, 2021)*, and issues with Ethereum may affect Oracle.

The article (Zhang, 2018) suggested that doctors have the confidence to access electronic records with patients. The authors focused on the effectiveness of not replicating the data stored on electronic medical records (EMR), but they proposed leaving control in the doctor's hands, as shown in Figure 6. The request starts from the patient; he makes an appointment at the hospital. Then the patient authorizes the doctor who has complete control of recording and sharing the patient's data if he likes. This technique puts the patient's electronic records in constant threat when the doctors are not trusted, and they behave maliciously and leak the patient's electronic records.

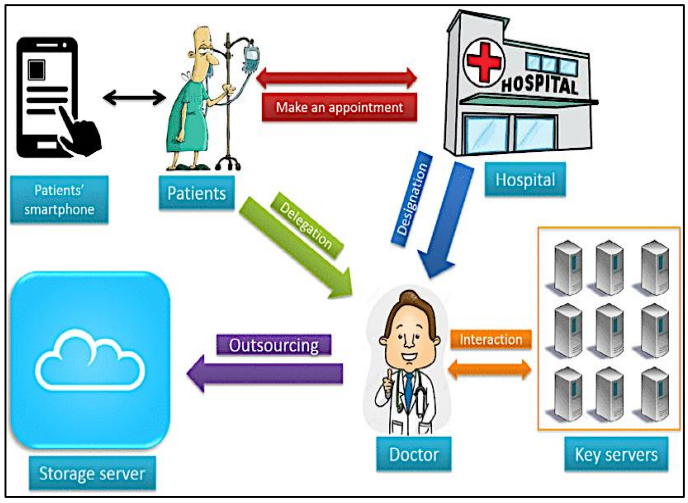

Figure 6: The system model proposed (Zhang et al., 2018)

Table 1 summarizes the critical techniques concerning centralization, third parties, and the patient's permission of his/her record independently.

Ref.	Approach	Centralized /Using Third Party	Patient Needs Authority to their EHR	Implementation	Year
Liang et al.,	Using medical coverage organizations as a third party	Yes	Yes	-	2017
Chen et al.,	Using a public cloud server as additional centralized storage	Yes	Yes	Python 2.7 and MongoDB	2019
Tanwar et al.,	Setting up and distributing servers as nodes	Yes	No	The python 3	2020
Tripathi et al.,	Using IoT based Wearable Devices on the patient	Yes	Yes	-	2019
Nguyen et al.,	Using a manager of electronic health records to encrypt and decrypt patient data	Yes	Yes	Java	2019
Sharaf & Shilbayeh	Operating a governmental authority as a central datastore	Yes	Yes	-	2019
Zhang et al.,	Giving doctors the authority to access HER	Yes	Yes	C language and MIRACL Library version 5.6.1	2018
Y. Zhuang et al., 2020	Setting up and distributing a local servers	Yes	Yes	-	2020
Madane et al., 2020	Using Oracle server as a primary centralized storage	Yes	No	_	2020

Table1: Comparison of security level with patient's permission to access his/her EHR independently

3. Research steps & approach

This research proposal is based on developing a Secure Electronic Health Record Model using blockchain technology patient has complete control over his/her EHR system. The high-level model is shown in Figure 7, consisting of different modules. The patient is an administrator to create the block of the medical record on a blockchain independently without involving any other entity. The main modules and phases of the proposed model are explained in the following:

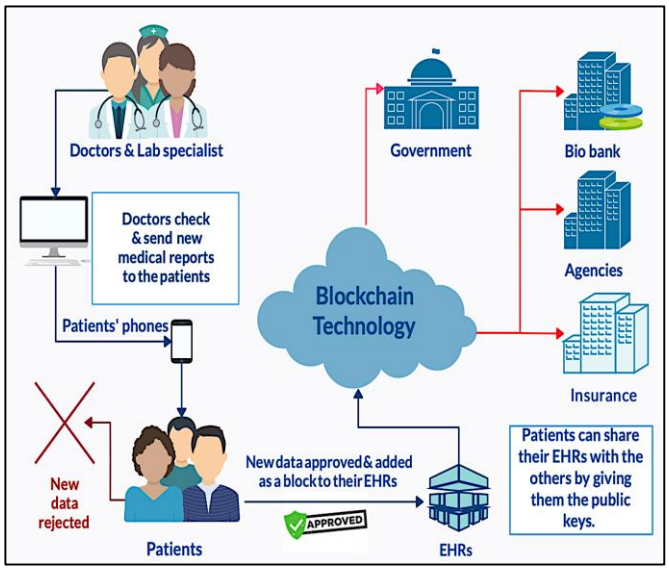

Figure 7: Blockchain-Based Secure Conceptual Framework of EHRs

A- Proposed Research Modules:

1- Doctor Module

The doctor will communicate with the patient after conducting the medical examination. The doctor will analyze the medical report received from the laboratory, X-ray, or image department and send the medical report to the patient.

2- Patient Module

In this module, when the patient receives the medical report, he/she can examine and have the authority to accept or reject the report. If the patient accepts his/her report, he can add this report into his/her HER by adding a new block on the blockchain system independently, and he/she has complete control, and the report is fully secured. The patient has another choice to reject the report, and it will not save in the blockchain system.

3- EHR Module

This module contains patient medical reports that the patient has added as new blocks in electronic health records for future reference. Later, the patient will add any new report in his/her EHR as figure 8.

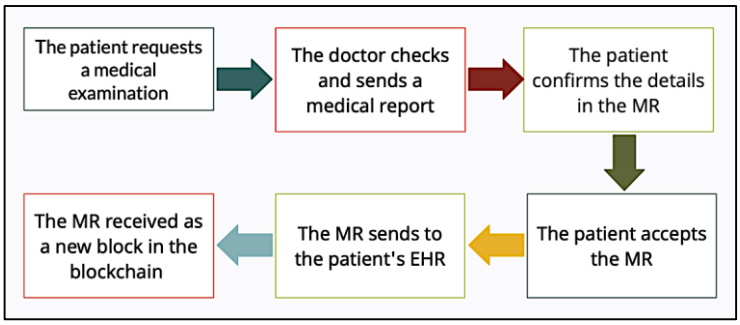

Figure 8: EHR Module

4- Government Agency Module

This module is related to accessing the medical record of a criminal patient if the government wants any verification. Sometimes there are issues directly related to patient records that require government intervention. That requires permission to access the patient's file. For example, prove a health condition for an official organization to obtain a sick leave or prove a health condition from any chronic disease to achieve a specific job. In addition, it can be adopted in some social issues, such as authorizing (premarital examination centers) to access specific data of applicants and ensure the compatibility of their genetic genes.

5- Biobank Module

Research centers for biological and medical data and biological samples rely on technology. So, we know that one of the essential advantages of blockchain technology is the decentralization of data with the ability to see some data in public without knowing the identity of the people, and this matter helps the possibility of using the Blockchain in studying the number of people with a specific disease and how to treat them, which helps reduce the number of expected infections for the general society. It helps in succession to reduce the enormous medical expenses around the world. In some cases, these research centers can communicate with the patients to request permission to access and view some more specific data.

6- Health Agency Module

Through international agencies such as the World Health Organization, the World Food, Drug Authority, and some regional and global agencies with a common interest to benefit from the health data contained within the blockchain nodes in the statistical and digital operations.

7- Insurance Module

Health insurance companies can know the health conditions of their customers by obtaining the public key for each client.

B- Research Phases

In the following section, we will discuss the essential phases of this research:

1) Literature Review

In this phase, the literature review of the use of blockchain technology in the health care field will be presented. The focus is to improve the security of electronic health records (HER) based on cloud storage servers. The detail of this part is presented in the Literature Review part of the proposal.

2) Secure EHR Design

The research-based is upon blockchain technology to protect electronic health records' security, privacy, and reliability. The patient has complete control of his/her medical record, and only the patient can give access to a doctor and others to view his medical history. Blockchain technology has many advantages such as distributed data storage, non-modifiable, non-penetrable, non-delete able. In the design phase, we will address the possibility of patient management of his health record without any other party. The abstract level Entity-Relationship (ER) diagram of system design is shown in figure 9.

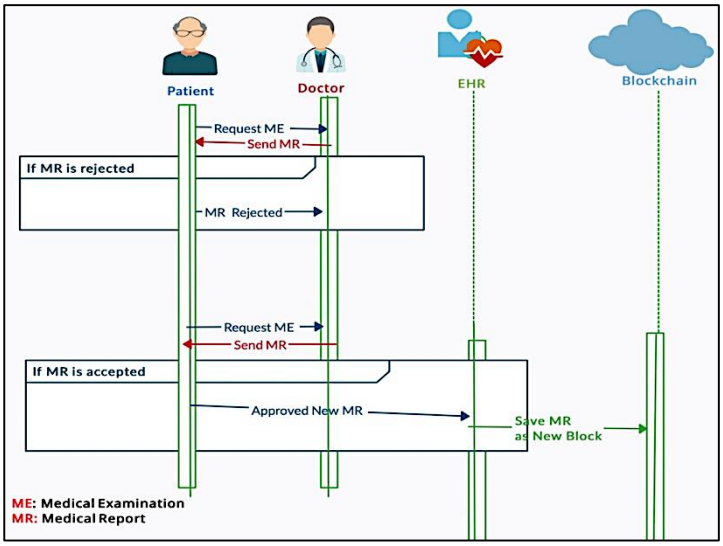

Figure 9: System Design ER Diagram

3) Secure EHR Implementation

This phase will describe implementing our proposed model. We will use the MATLAB tool to implement our prototype model, which consists of the following six scenarios:

I. The patient and the doctor will sign up for their account.

II. The doctor and patient will sign in to their accounts, and the patient will fill up his/her account with data such as age, health, situation, and any disease he/she has.

III. The doctor will conduct the necessary medical examination to diagnose the patient's health condition,

write the appropriate prescription for him/her, and will send it to the patient.

IV. The patient logs in and adds the username of the doctor who prepares the medical report.

V. The patient's medical report appears on the system, which contains:

a. Doctor's and the patient's names.

b. Medical diagnostic data and doctor's notes.

c. The appropriate medical prescription for the patient's condition.

VI. After examining the entire report, the patient has one of two options:

a. Choose (Accept) to add the Medical Report to his EHR on the Blockchain if he is sure of the integrity of the data and matches it to his expected condition.

b. Choose a rejection to refuse that report in the event of incorrect or any other data issues.

4) Research Limitation

The limitation of this research is the application of the proposal to algorithms and approaches using MATLAB compared to its implementation on an integrated system that contains (nodes) and an authentic experience for patients through their receipt of medical reports and their acceptance to be uploaded on their Blockchain. Respectively, an integrated system takes more time and the approval of official authorities Cooperative and the presence of volunteers as patients.

A simulation was created as a platform that connects doctors and patients through which they sign up an account through which the doctor can describe the health status after diagnosis and write the prescription for that.

Figure 10: The result of implementing Main of the Blockchain

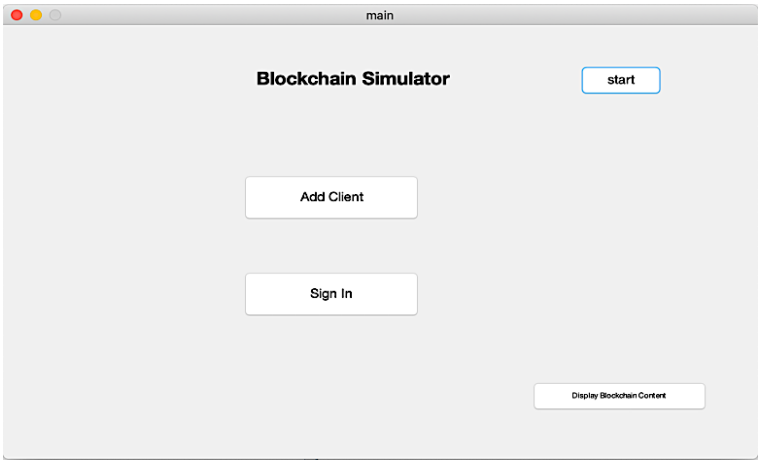

Figure 11: After pressing the start button, we must register as new patients and doctors.

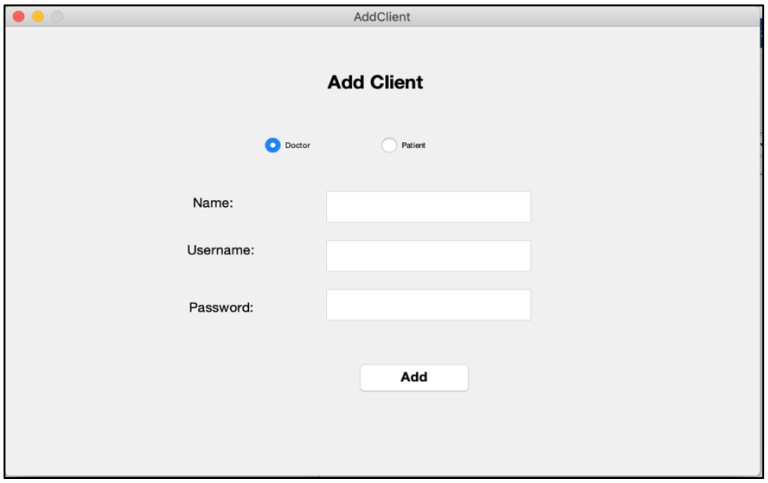

Figure 12: doctors and patients sign up through this window.

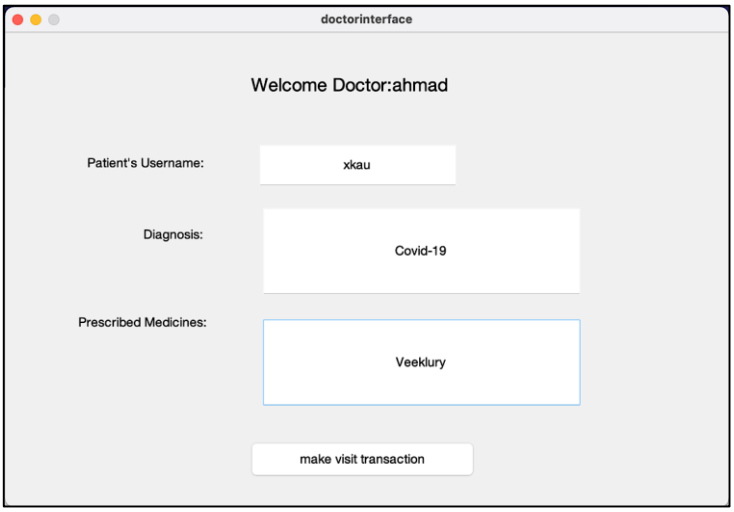

Figure 13: Here, the doctor's interface fills up the patient's username, diagnosis, and prescribed medicines.

Patient signs in and write down the doctor's username and press (Show Waiting Visits) Figure14. Then the patient can accept the diagnosis or leave it as rejection in the waiting visits.

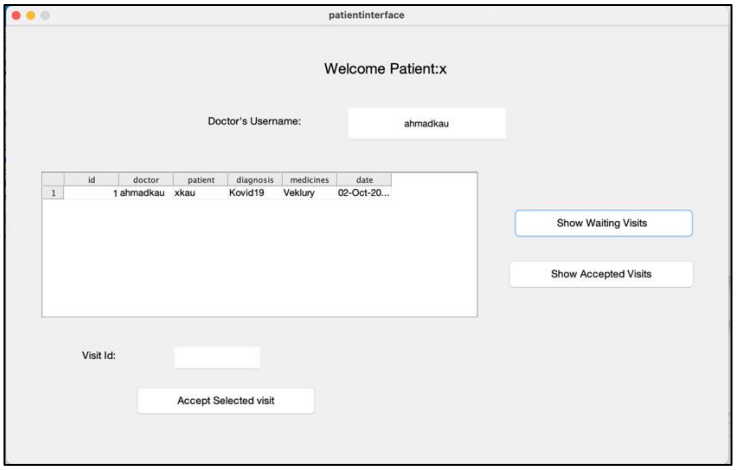

Figure 14: Patient's Interface

4. Results & comparison

I. INTRODUCTION

The introduction of the Blockchain in the healthcare sector is primarily about increasing security and improving data protection. In addition to the possibilities of the Blockchain for doctors, authorities, and patients, the interaction of the data flow between patients and hospitals or service providers in the healthcare sector can also be significantly improved. The Blockchain can be an ideal solution wherever information has to be stored and passed on. Blockchain also plays a significant role when companies exchange data from patients in the healthcare sector, as it improves data protection and the security of transmission.

The Blockchain decentralizes health information and thus increases efficiency. No central storage is necessary, as the data is decentralized by the individual companies and people involved. It is one of the most significant advantages of the Blockchain, parallel to the security against manipulation, encryption, and the constant control and transparency of all data.

II. Security

Hash function: We use DataHash to hash data information on the Blockchain. In this function, we set hashing method to SHA-256. In the Blockchain, a hash function is used in various situations. A hash function is a function that has the following characteristic properties. • Returns fixed-length output data from arbitrary length • SHA-256 can only convert some data in one direction, and it is impossible to convert hashed data back to the original data. SHA-256 is a one-way function, and there is no reversal mechanism. This function is computationally

Input Data				Hash Output SHA-256
Patients ID	Dr. ID	Diagnosis	Prescription	
14220	78792	Severe headache	pain reliever	previousHash: '075c27741a3506846368fa6e5b3477f85b31ceee71a5716e2f12b40fa21d23aa' selfHash: '001b79bd0771f5b708ddaa9af2e37509'
14220	78792	Gout	ibuprofen	previousHash: '001b79bd0771f5b708ddaa9af2e37509' selfHash: '002e03786ec3513864f761291e8850e0'
14220	78792	Severe headache	Anti-inflammatory	previousHash: '002e03786ec3513864f761291e8850e0' selfHash: '00034a16769fa1a2dda68c14e13bd01e'
14220	78792	Renal colic	corticosteroids	previousHash: '00034a16769fa1a2dda68c14e13bd01e' selfHash: '0084008244f18e4ee6f1961535eee194'
33001	78792	diabetic	insulin syringe	previousHash: '0084008244f18e4ee6f1961535eee194' selfHash: '00e43bc43216d5aadb0e86bf7669e094'

Table 2: SHA-256 Hash function output

effective, and a computer with an average specification can operate hundreds of times per second. Table 2 shows the result of using a cryptographic hash function to EHR data.

III. Efficiency

It is essential to evaluate the system performance related to scalability and efficiency concepts we need to the data integrity proof generation, so we test our system with different numbers of concurrent records in a range from 1 to 10,000 with the help of 'tic' and 'toc' MATLAB methods to measure the time elapsed for creating a new record in the system Figure 15.

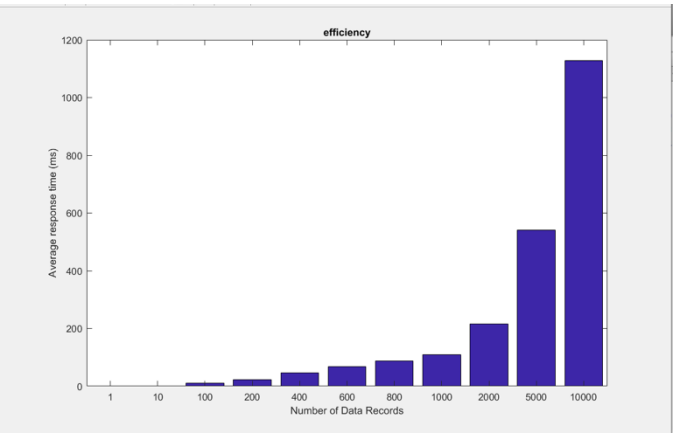

Figure 15: Graph of number record versus average response time

From this figure, we notice that the system can handle a large dataset at low latency, indicating the data process's scalability and efficiency.

IV. Capacity

We can explain the meaning of (block capacity) as adding a new block to the previously existing group of blocks in the Blockchain to serve as a database and record the ledger in an encrypted way through data structures called blocks. These blocks are mainly used as data units used to store transaction information for the network. The first block is called the Genesis block, as there is no previous block for it as a new chain. Block capacity is also sometimes calculated as the current length of the Blockchain minus one. The first block has no height but a size. We calculate the capacity of the block array with the increasing number of blocks in Tables 3,4, and fig 16.

numblock	size of blocks
1	8 b
100	808 b
200	1.57 kb
300	2.35 kb
400	3.13 kb
500	3.91 kb
600	4.70 kb
700	5.48 kb
800	6.26 kb
900	7.04 kb
1000	7.82 kb
1100	8.60 kb
1200	9.38 kb
1300	10.16 kb
1400	10.95 kb
1500	11.73 kb
1600	12.51 kb
1700	13.29 kb
1800	14.07 kb
1900	14.85 kb
2000	15.63 kb
2100	16.41 kb
2200	17.20 kb
2300	17.98 kb
2400	18.76 kb
2500	19.54 kb
2600	20.32 kb
2700	21.10 kb
2800	21.88 kb

Table 3: capacity of blocks (part1)

2900	22.66 kb
3000	23.45 kb
3100	24.23 kb
3200	25.01 kb
3300	25.79 kb
3400	26.57 kb
3500	27.35 kb
3600	28.13 kb
3700	28.91 kb
3800	29.70 kb
3900	30.48 kb
4000	31.26 kb
4100	32.04 kb
4200	32.82 kb
4300	33.60 kb
4400	34.38 kb
4500	35.16 kb
4600	35.95 kb
4700	36.73 kb
4800	37.51 kb
4900	38.29 kb

Table 4: capacity of blocks (part2)

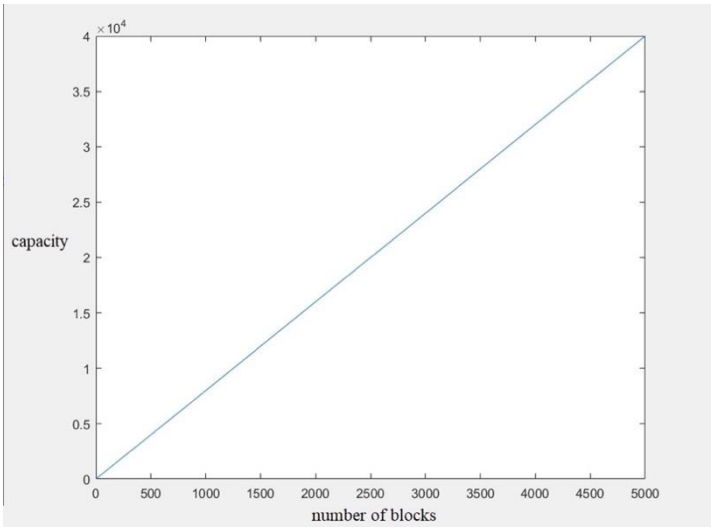

Figure 16: Graph result of the number of blocks versus capacity in byte

V. *Comparison*

The implementation results are compared with the well-known existing techniques that have been discussed in the literature review. The proposed compared our results with the following two approaches presented in the two papers published on cloud-based EHR solutions. The comparison focuses on the features of our research proposal with two EHR cloud-based management solutions (Zarezadeh, 2020) and (Wang, 2019) , as shown in table 4, to give the patient control over his electronic health record, distributed database storage.

Aspect	(Zarezadeh et al., 2020)	(Wang et al., 2019)	Our Proposal
Distributed	No	No	Yes
Patient control of HER	No	No	Yes
Immutable	No	No	Yes
Removable	Yes	Yes	No
Using Third-Party	Yes	Yes	No

Table 5: Comparison of our research suggestion with two techniques

5. Conclusion and Future work

As we have indicated in previous papers, we find that some of them recommend relying on some intermediary companies such as Oracle and Ethereum, all which conflict with the ultimate blockchain mechanism. Some papers recommend relying on certain parties as intermediaries, which has proven their limitations and centralization, which goes against the principle of Blockchain.

This proposal recommends giving the patient the authority to accept the medical report as a new block to the patient's Blockchain. Moreover, the proposal recommends independence (Node) from private for-profit companies such as Oracle and Ethereum to avoid any negative consequences in the future. The proposal recommends the creation of a (node) within each medical city to form a global, non-profit network whose establishment will be pursued under the supervision of technical scientists and doctors from around the world for transparency, credibility, and integrity.

References

Adlam, R. &. (2020). A permissioned blockchain approach to electronic health record audit logs, in 'Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications'. *Association for Computing Machinery*, 1-7.

Caldarelli, G. &. (2021). The blockchain oracle problem in decen- tralized finance—a multivocal approach. *Applied Sciences*, 11 (16), 7572.

Wiljer, D. a. (2019, 08 02). *Bringing blockchain to healthcare for a new view on data*. Retrieved from IBM: https://www.ibm.com/blogs/think/2019/08/bringing-blockchain-to-healthcare-for-a-new-view-on-data/

Cao, S. Z. (2019). Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain. *Information Sciences*, 485, 427–440.

Chen, L. L.-K.-C.-K. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems* , 95, 420–429.

Wackerow, P. (2021, 08 0). *GAS AND FEES*. Retrieved from Ethereum: https://ethereum.org/en/developers/docs/gas/

Ethgasstation. (2021, 12). *ETH25 LEADERBOARD*. Retrieved from ethgasstation: https://ethgasstation.info

McDermott, K. &. (2020). Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*, 10(4), 48–53.

Kamerer, J. L. (2020). Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*, 10(4), 48–53.

Liang, X. Z. (2017). Integratingblockchain for data sharing and collaboration in mobile healthcare applications. *IEEE*, 1–5.

MacKenna, B. B. (2020). Impact of electronic health record interface design on unsafe pre- scribing of ciclosporin, tacrolimus, and diltiazem. *Journal of Medical Internet Research*, 22(10), e17003.

Simonton, O. C. (1992). Getting well again: A step-by-step, self-help guide to overcoming cancer for patients and their families. *Bantam*.

Madine, M. M.-H. (2020). Blockchain for giving patients control over their medical records. *IEEE*, 8, 193102–193115.

Nguyen, D. C. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access* , 7, 66792–66806.

Sharaf, S. (2019). Asecureg-cloud-basedframeworkfor government healthcare services. *IEEE Access* , 7, 37876–37882.

ethereum.org. (2021). *Nodes and clients*. Retrieved from ethereum.org: https://ethereum.org/en/developers/docs/nodes-and-clients

Sharma, Y. &. (2020). Preserving the Privacy of Electronic Health Records using Blockchain. *Procedia Computer Science*, 173, 171-180.

Shamshad, S. M. (2020). A secure blockchain-based e-health records storage and sharing scheme . *Journal of Information Security and Applications*, 55, 102590.

Shi, S. H. (2020). Applications of Blockchain in ensuring the security and privacy of electronic health record systems: A survey . *Computers & Security*, 97, 101966.

Singh, S. P. (2020). Three-dimensional printing in the fight against novel virus COVID-19: Technology helping society during an infectious disease pandemic. . *Technology in society*, 101305.

Tanwar, S. P. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. . *Journal of Information Security and Applications*, 50, 102407.

Tripathi, G. A. (2019). S2HS- A Blockchain-based approach for smart healthcare system. . *Healthcare*, 100391.

Verizon. (2019). Data Breach Investigations Report. *Computer Fraud & Security*, 4.

Vora, J. I. (2018). Ensuring Privacy and Security in E- Health Records. Paper presented at the 2018 International Conference on Computer. *Information and Telecommuni*, 11-13.

Vora, J. I.-1. (2018). Ensuring privacy and security in e-health records. *International conference on computer, information and telecommunication systems (CITS)* (pp. 1-5). -: IEEE.

Wang, X. B. (2019). A dual privacy-preservation scheme for cloud-based eHealth systems. *Journal of Information Security and Applications*, 47, 132–138. .

Y. Zhuang, L. R.-W.-Y.-R. (2020). "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," . *IEEE Journal of Biomedical and Health Informatics*, 2169-2176, A.

Zarezadeh, M. T. (2020). Attribute-based Access Control for Cloud-based Electronic Health Record (EHR) Systems. . *IseCure*, p126-140, 12p.

Zhang, Y. X. (2018). HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems. *IEEE Transactions on Industrial Informatics*, 14(9), 4101-4112. .