Hindawi
Security and Communication Networks
Volume 2023, Article ID 9856473, 1 page
https://doi.org/10.1155/2023/9856473

Retraction

Retracted: Electronic Health Record Monitoring System and Data Security Using Blockchain Technology

Security and Communication Networks

Received 5 December 2023; Accepted 5 December 2023; Published 6 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] K. T. Akhter Md Hasib, I. Chowdhury, S. Sakib et al., "Electronic Health Record Monitoring System and Data Security Using Blockchain Technology," *Security and Communication Networks*, vol. 2022, Article ID 2366632, 15 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 2366632, 15 pages
https://doi.org/10.1155/2022/2366632

Research Article

Electronic Health Record Monitoring System and Data Security Using Blockchain Technology

Kazi Tamzid Akhter Md Hasib,[1] **Ixion Chowdhury**,[1] **Saadman Sakib**,[1] **Mohammad Monirujjaman Khan**,[1] **Nawal Alsufyani**,[2] **Abdulmajeed Alsufyani**,[2] **and Sami Bourouis**[3]

[1]*Department of Electrical and Computer Engineering, North South University, Bashundhara, Dhaka 1229, Bangladesh*
[2]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[3]*Department of Information Technology, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*

Correspondence should be addressed to Mohammad Monirujjaman Khan; monirujjaman.khan@northsouth.edu

Received 12 October 2021; Revised 24 November 2021; Accepted 13 January 2022; Published 4 February 2022

Academic Editor: Chinmay Chakraborty

Bangladesh should have owned a decentralized medical record server. We face a lot of issues, such as doctor's appointments, report organization in one spot, and report follow-ups. People now bring a large number of papers to the doctor's chamber. They carry prescriptions, reports, and X-ray files, among other things. It complicates everyone's life as a result. All of the reports must be reviewed by doctors on a regular basis. It is difficult to read old reports on a regular basis, and patients do not receive the correct medications or treatment. Doctors also find it extremely difficult to comprehend handwritten prescriptions. Data security, authenticity, time management, and other areas of data administration are dramatically improved when blockchain (smart contract) technology is linked with standard database management solutions. Blockchain is a groundbreaking, decentralized technology that protects data from unauthorized access. After smart contracts are implemented, the management will be satisfied with the patients. As a result, maintaining data privacy and accountability in the system is tough. It signifies that the information is only accessible to those who have been authenticated. This study focuses on limiting third-party engagement in medical health data and improving data security. Throughout the process, this will improve accessibility and time efficiency. People will feel safer during the payment procedure, which is the most significant benefit. A smart contract and a peer-to-peer encrypted technology were used. The hacker will not be able to gain access to this system since this document uses an immutable ledger. They will not be able to change any of the data if they gain access to the system. If the items are found to be defective, the transaction will be halted. Transaction security will be a viable option for recasting these problems using cryptographic methodologies. We developed a website where patients and doctors will both benefit because of the use of blockchain technology to ensure the security of medical data. We have different profiles for doctors and patients. In the patient profile, they can create their own account by using a unique address, name, and age. This unique address will be created from the genesis block. The unique address is completely private to the owner, who will remain fully secure in our network. After creating an account, the patient can view the doctors' list and they can upload their medical reports such as prescriptions and X-rays. All the records uploaded by the patient will be stored on our local server (Ganache). The records are stored as hashed strings of the data. Those files will also have a unique address, and it will be shown in the patient profile. After granting access, the doctors will be able to view their records in the respective doctor's profile. For accessing the options such as uploading, viewing, or editing the data, Ethereum currency (a fee) will have to be paid in order to complete the request. On the other hand, doctors can enter their profile using their name and unique address. After logging in, they can view their name, unique address, and the list of patients that have granted access to the doctor to view their files. On our website, the front end is handled by JavaScript, ReactJS, HTML, and CSS. The backend is handled by Solidity. Storage is handled by Ganache as the local host. Finally, this paper will show how to ensure that the procedure is as safe as feasible. We are also maintaining transparency and efficiency here.

1. Introduction

The electronic health record is called an EHR. As we know, we are heading towards the fourth industrial revolution. For that, we need to be ready to tackle data. In the modern world, data are an asset. Moreover, medical data is so important and it has security issues as well. Every system cannot handle this security. Critical data in today's global market has a huge impact on the worldwide economy. In the modern world, the revolution in EHRs (electronic health records) has changed medical care and management drastically. People could not access their medical data from their devices before. Because of this system, people from all over the world can access their medical data through websites. We made a website that has some revolutionary features, including doctors' and patients' different profiles. They can interact with each other using the blockchain network. A simple blockchain system can be defined by an ordered list of the nodes and links that are used, with these nodes having the ability to store information and chains connecting these links [1]. The block contains the data. It ensures the privacy of the data. Every block is integrated with each other. No one can temper the medical data easily, either. According to the blockchain security ecosystem, the confidence is based on the increased security, better transparency, and immediate traceability provided by blockchain technology. Beyond issues of trust, blockchain provides a slew of other business advantages, including cost savings as a result of improved speed, efficiency, and automation, among other things. Blockchain lowers overhead and transaction costs substantially by decreasing or eliminating the requirement for third-party or middle-man verification of transactions. Blockchain does this by drastically reducing paperwork and mistakes. The medical record systems currently used by healthcare institutions are highly susceptible to alteration, fabrication, and the risk of getting lost. Additionally, a patient with a long history of medical complications may face the hassle of having to carry a lot of reports to their doctors. Healthcare institutions may record their patients' information digitally, but it will always require a person to verify and insert it into their database. This is an unreliable way of managing such sensitive information. The whole system of record keeping requires patients to travel from one help desk to another to get the information they require. These issues are neglected and some are considered standard protocol in our healthcare industry. Moreover, there are incidents where doctors have prescribed wrong medications based on an unverified report or a patient has had to return without receiving consultation because they forgot to bring certain reports [1–4].

In [5], the authors discussed that to validate and store data, blockchain technology employs blockchain data structures. The data received from the end user are first encrypted so that it is only visible to them. It is then verified and added to blocks in a decentralized system, ensuring data security and accessibility. The data are stored in a block in key and value pairs where each of the blocks is well interconnected to each other. The system is alerted when one of the data contained in the blockchain is tampered with, and the blocks become fragmented. Moreover, all the data stored in the blockchain will be completely transparent to all entities while being encrypted. No one can view them unless the owner gives permission for it. The authors of the paper [6] emphasized that they solved the health record system because it was difficult to monitor and protect against potential threats. The writers have taken the distributed computing idea of blockchain and adapted it to a variety of applications. They highlighted a few of the potential uses for this kind of decentralization. This technology is becoming more widely used, and its primary use is data exchange, which includes access control and administration of patients' medical information. We analyzed one existing similar system and found the author [7] mentioned a cloud-based medical record system that encrypts medical data using the ABE method. These records describe the patient's condition without revealing the exact nature of the disease or the doctor's location. In reality, the article uses symmetric encryption, but one of the strategy's fundamental weaknesses is that it relies on a perfectly trustworthy global authority to handle key management, issue public system settings, and generate secret keys for the doctor. To aid the network in achieving an agreement, the method depends on a single centralized point of trust for transactions. A technique for constructing a conceptual framework for a medical health record management system is included in the study. Its main aim is to guarantee safe transactions by using blockchain and smart contracts.

In [8], the authors figured out that a blockchain is an ever-growing collection of data known as cryptographically linked and secured blocks that are cryptographically linked and protected. Cryptography is used to connect the blocks. The bulk of nodes in the blockchain network are in charge of block verification. When we go further, there are a few traits that distinguish blockchain from other technologies. Data stored on the blockchain, for example, are immutable, tamper-resistant, and based on a decentralized network, so it cannot be hacked or decoded in any way. In general, there are three sorts of blockchain: public (or unapproved), private (or allowed), and consortium (or both private and allowed) (or permitted). As a consequence of the network's geographically varied geographic area, each one has its own distinct characteristics. Smart contracts, according to [9] Nick Szabo, are "a computerized transaction protocol that complies with contract conditions." Smart contracts are code snippets written in a high-level programming language that are used to complete transactions (software or scripts). There are programming languages such as Java, C++, Python, NodeJS, Go, and Solidity. Many blockchain systems utilize a variety of high-level programming languages to create smart contracts.

In [10], the authors indicate that between 2013 and 2014, the number of office-based physicians who utilize certified electronic health record systems increased. In 2014, 74.1 percent of office-based physicians utilized a certified EHR

system. According to the findings of the study, 56.8% of doctors in Alaska and 88.6% of doctors in Minnesota utilize a certified EHR system. The HITECH Act of 2009 offered monetary incentives to qualified physicians who used a certified electronic health record system, which may be one of the reasons for the continued rise in physician usage of these systems. According to the American Medical Association, physicians who utilized a certified EHR system shared patient information with clinicians outside their medical group in 2014.

The authors discussed in [11] that electronic health records (EHRs) are used for research all around the globe. The ability to analyze real-world real-patient results in near-real time, which is not feasible with other techniques, is a clear and unique benefit. Whether done prospectively or retrospectively, the cost and convenience of evaluating existing data are less expensive and more convenient than the cost and convenience of creating a human-curated dataset. The future potential for EHR in research seems to be almost unlimited, especially as the types of data collected and the ability to extract information from records continue to improve. The EHR is being gradually changed and upgraded to make research more accessible as the usage of electronic health data for research increases in popularity. The North American Association of Central Cancer Registries and the Standards for Oncology Registry are attempting to establish data format and display standards, as well as common data components, such as the National Cancer Institute. Structured data, according to E. Kim and colleagues, is more likely to contain this information. It may be found in the story (+/machine comprehensible). It is unlikely that it will show up in EHR Facts and Statistics [12].

In [13], the authors showed that the International Data Encryption Standard Algorithm (IDEA) with salt will be used to protect patient-sensitive data during transmission. The session will be protected via the usage of JSON Web Tokens, which internally use the Signature Algorithm HS256. The SHA256 algorithm with salt will be used to protect the confidentiality of passwords. Everything done so far is towards at protecting electronic medical data (EMD) against external theft. Providing integrity and privacy for sensitive data does not just relate to external invaders but also applies to data leaks that may occur inside an organization. In [14], the authors emphasize that blockchain technology is at the heart of data acquisition since it guarantees the integrity and dependability of information. Tamper-proof and open class verification features guarantee that the information on the block cannot be tampered with in any way. Even if the attacker altered part of the ledger information, the system would detect and fix the error in a short period of time. In order to create network congestion, the authors also said [15] an adversary may attempt to submit a large number of requests to endorsers at the same time. In some ways, it is comparable to denial of service (DoS) assaults. It serves no purpose since the endorser only responds to client requests by verifying that the data have been signed by the client. Even if the expense is huge, the impact is small. Additionally, nodes in the system may be attacked, crash, or even turn against one another. The consensus process and the election of endorsers may both help to maintain the stability of the system and reduce the likelihood that opponents will do significant harm. In addition to ensuring data privacy, the access control mechanism on the ledger may provide results similar to those obtained via ring signatures and zero-knowledge proof. A highly effective method of protecting the privacy of patients is through the use of encryption. In [16], the authors mentioned that our proof-of-stake method, which incorporates implicit bonding, makes it simpler to audit each entity's involvement in the system while simultaneously giving large payers (such as the Centers for Medicare and Medicaid Services) a simple option to promote participation. In reality, during the time of image collection, the institution provides resources for the study. In [17], the authors also discussed how the peer-to-peer network of nodes and associated blockchain architecture are design decisions that effectively address another interoperability criterion: the sharing of protected health information (PHI) with patient-authorized recipients over a secure, private, and tamper-resistant network infrastructure. As previously mentioned, the chaining technique produces an effectively immutable data record, meaning that any attempt to change existing blocks will be immediately visible to the observer.

In [18], the authors described how MetaMask is also used to store patient and healthcare provider keys. MetaMask is a bitcoin wallet that works with Chrome, Firefox, and Microsoft Edge. MyEtherWallet and MyCrypto are two more cryptocurrency wallets. MetaMask's goal is to make connecting to the Ethereum network as easy, reliable, and secure as possible. Furthermore, since its inception in 2016, MetaMask has not been hacked severely. MetaMask has become a useful tool in our work. In this article, we present a system that satisfies the security, privacy, interoperability, and performance requirements of an EHR system. Patient data may be shared anywhere and at any time using the recommended method as long as the patient grants permission. Only a few authors [19] have shown that the aforementioned EHR system criteria are covered by existing research. However, all of these criteria are taken into account in this project to guarantee patient data security and privacy, interoperability, and performance needs are met. To fulfill these criteria, our study employs blockchain technology, which employs a sophisticated and long-lasting cryptographic technique to allow cross-healthcare-provider data exchange while giving patients ownership over their information. The goal of the study is to create and evaluate a blockchain-based electronic health record application for security, privacy, interoperability, and performance. The authors [20] suggest a method for electronic transactions that does not depend on the confidence of the participants. As a starting point, we used the traditional structure of coins created using digital signatures, which offers tight control over ownership but is insufficient since it lacks a mechanism to prevent double-spending. A proof-of-work network, which records a public history of transactions and makes it computationally difficult for an attacker to alter the history if honest nodes hold a majority of CPU power, was suggested to address this challenge. Because of its unorganized

simplicity, the network is very durable. Nodes operate in a synchronous fashion with minimal cooperation. They do not need to be identified since communications are not directed to any specific location and simply need to be delivered using the best available technology. With the help of this consensus mechanism, all necessary regulations and incentives may be implemented [21]. PHR described it has a straightforward interface that allows you to quickly go through the following options: appointments give you the freedom to schedule appointments with your physician and canceling them before the appointment if necessary. A directory of your medical history, medicines, allergies, and vaccination records is kept in your health history file. It is simple to view the records of claims that have been filed on your behalf when you use the Claims History feature [22]. Furthermore, [23] by providing you with a database containing all of the lab findings for the tests you have performed, you may save both time and effort on your part. Connecting with your provider through direct and secure messaging is made possible by secure messaging services. Demographics: it allows you to make changes to any of your personal information, such as your phone number or address.

We also notice that [24] cloud-based electronic health record platform, GenexEHR, was developed to assist clinics and hospitals in managing patient data, thus allowing informed choices. Developed with the patient in mind, this platform assists in the preservation of the patient's health information across several healthcare settings. Using its state-of-the-art healthcare software, Genex HI, hospital management and information solution, meets the software and workflow needs of hospitals, clinics, and even individual patients. GenexEHR, Inc., provides Software-as-a-Service Laboratory and Clinic Management software. It is possible that latency will be impacted if there is an excessive amount of data. Because of the low storage and computing needs, blockchain transactions will be extremely cost-effective in terms of storage and processing. Another method of increasing performance is using decentralized databases such as BigchainDB and HBasechainDB. In the case of a large-scale deployment, the system may also contain tracking devices as well as extra actors. The quantity of data that can be stored on the blockchain is growing, so we may need to use off-chain architecture to store the original data while keeping the evidence of existence on the blockchain. There is a possibility that this may become a future study subject for this inquiry [25].

In this paper, we created a website that benefits both patients and physicians since we are using blockchain technology to guarantee the confidentiality of medical data. Our website has distinct profiles for physicians and patients. They may establish their own account under the patient profile by providing a unique address, name, and age. This one-of-a-kind address will be generated from the genesis block and cannot be entered into anyone's profile. The owner's unique address is totally confidential and will stay completely safe in our network. After establishing an account, the patient may see a list of physicians and upload medical records such as prescriptions and X-rays. All of the patients' submitted records will be kept on our local server (Ganache). The records are kept in the form of hashed strings containing the data. Additionally, each file will have a unique Uniform Resource Locator (URL) that will be shown in the patient's profile. There will also be an option for patients to give physicians access to their medical records. After being granted access, physicians will be able to see their records in their profile. To get access to features such as uploading, viewing, or modifying data, Ethereum money (a charge) will need to be paid. Doctors, on the other hand, may create a profile using their name and a unique address. They may see their name, unique address, and a list of patients who have given the doctor permission to read their files after signing in. The front end of our website is powered by JavaScript, ReactJS, HTML, and CSS. Solidity manages the backend, while Ganache acts as the local host. Finally, this article will show how to preserve the method's safety while simultaneously preserving its transparency and efficiency.

Section 1 explores and briefly explains blockchain, cryptocurrency, and smart contracts. Section 2 includes a description of the technique and materials used, as well as a discussion of the issues and a diagram of the entire system and how it all works together. The findings and analysis, as well as a comparison of the EHR to current systems, are presented in Section 3. Finally, Section 4 discusses the conclusion and future prospects.

2. Method and Materials

Healthcare institutions' existing medical record systems are extremely vulnerable to modification, falsification, and the possibility of data loss. Additionally, a patient with a lengthy history of medical problems may have to deal with the inconvenience of having to bring a large number of reports to their doctor's appointments. Healthcare organizations may choose to digitize the information they collect about their patients, but a human will always be required to verify and enter the information into their database. When dealing with such sensitive material, this is an untrustworthy method of handling it. Under the current record-keeping system, patients are required to go from one help desk to another in order to get the information they need. The majority of these problems are ignored, and some of them are even considered normal practice in our healthcare sector. Furthermore, there have been instances in which physicians have given incorrect medicine based on an unconfirmed report, or in which a patient has been required to return without getting consultation because they failed to bring the necessary papers with them to the appointment. Blockchain technology makes use of blockchain data structures in order to verify and store data. The information received from the end user is first encrypted in order to ensure that it is only accessible to that individual. Data security and accessibility are ensured in a decentralized system by having it validated and added to blocks in a decentralized system. The data are kept in a block in key and value pairs, with each of the blocks being properly linked to the previous and following blocks. When one of the data blocks in the blockchain is tampered with, the system receives an alert. If the blocks become

fragmented, the system is notified. Furthermore, all data saved in the blockchain will be fully visible to all entities while also being encrypted so that no one will be able to see them until the owner grants permission for them to be viewed by others. A blockchain-based system for storing and retrieving medical data will make the whole process of updating, retrieving, and displaying medical data much more frictionless. As a result, inside the blockchain architecture, the hospital's activities might be viewed as information services. In a blockchain-driven cyber environment that resembles real-world EHR operations, smart contract design may thus be viewed of as the computation of start and finish times for information services.

2.1. Outline of Full System. Figure 1 shows the EHR architecture of the proposed system in this paper. The primary users in the blockchain architecture are a doctor, a patient, and a hospital. Furthermore, in the blockchain ecosystem, everyone will have a unique power due to the system's own private keys. Doctors, patients, and hospitals may also have limited access to some functionalities. Using his or her private key, the doctor will gain access to the web app (Frontend). By using his own private key, the patient communicates with the doctor. Both parties will share medical information via a web app (Frontend). Patients must use a smart contract to transact after receiving the service. As a backend support, we are deploying the Ethereum network. Below, the roles of every character in this figure are described:

(1) Doctor: doctors can access the system by using a private key, which will be given by the patient's unique key.

(2) Patient: patients will provide private key to doctors. Patients can share personal data through our portal.

(3) Hospital: hospital admin can look into the process but not details. They can maintain the flawless communications system.

(4) Website: the website is under frontend programming. It connects with the backend through smart contracts.

(5) Smart contracts: It is the main bone of our system. Every change in a block will have a log in it.

(6) Ethereum network: for backend processing, we used the Ethereum network.

2.2. Process of System. Figure 2 shows that the patients must first visit the hospital for a doctor's consultation. Both the patient and the doctor must have a network account. A new patient must first register an account and fill out his or her profile's primary information. After filling out the form, the doctor will search the network for his or her information and consult with the patient. The hospital will update the patient's information on the blockchain network after checking with the doctor. So, all the processes are connected to the blockchain network with websites.

As shown in Figure 3, the hospital has access to the patient's public key, but only the patient has access to his or her own private key. If a doctor wishes to see a patient's medical records, he or she must make a request to the patient. When the patient receives the queue request in his mobile app or on his website, he or she can authorize access by inputting their private key. After the operation is completed, the blockchain network will be updated.

Figure 4 shows an example of an unauthorized user cannot access the EHR application focused on the patient since the patient's data must demonstrate its security. The SHA-3 (Keccak-256) hash, which generates a 64-character hexadecimal string, can be used to get access to the program. The patient's public key is used to encrypt each transaction and can only be decoded with the patient's private, encrypted key, thanks to cryptography. The elliptic curve digital signature algorithm protects all nodes on the Ethereum network (ECDSA).

The functions of individual entities are depicted in Figure 5. When we look into the node in our network, we observe blocks and blocks are interconnected in the blockchain network. A block, as shown in the diagram above, consists of two parts: a block header and a block body. A ledger is a collection of linked blocks. The patient's public key is contained in each block. The preceding transaction's hash, the encrypted data hash, and the service provider's digital signature must all be provided. A copy of the blockchain ledger will be sent to each node in the network. Inside every block, there is some mechanism of the blockchain ecosystem. In the block header, there is a previous block hash, signature, root hash, timestamp, and nonce. We have described it all before. Inside the block body, we have found the root hash. Every root is interconnected with every block. We see that Tx1. Tx1 means 1 transaction happened, and so, we found the hospital, doctor, diagnosis, date, and signature as it is unique.

Figure 6 shows the entire system's entity relationship (ER) diagram. We concentrated on patient, doctor, and lab report storage. First and foremost, the patient can visit the websites and create an account. Users can register and choose a hospital, but we are only proposing one. The user can view their prescription history as well as other medical information. In the future, new features will be added to our project's tasks. If we see the main features in the figures, they are the patient, doctor, and laboratory. Patients are connected with Login, Signup, Select Hospital, View Past Records, and Make an Appointment. We introduced patients to doctors by providing them with treats. Doctors are linked with the ability to view appointments, diagnose patients, make appointments with patients, and also add lab tests. Doctors are interconnected with laboratories. Because he/she can make decisions for patients, they can tell a patient if a lab test is mandatory or not. We discovered that we can view the lab test, generate a lab test report, and perform lab tests using the lab test.

Figure 7 shows the login page. It is for both the doctor and the patient. Both must fill in their names and log in by address to their respective accounts in order to log in. You can create three distinct sorts of accounts on this page. The

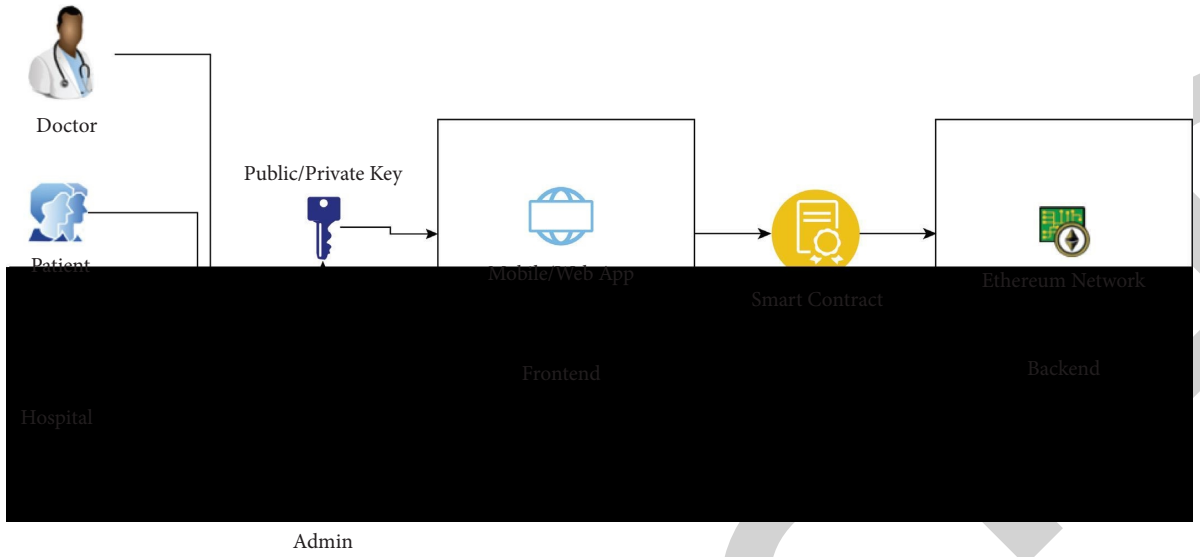

Figure 1: EHR architecture of our system.

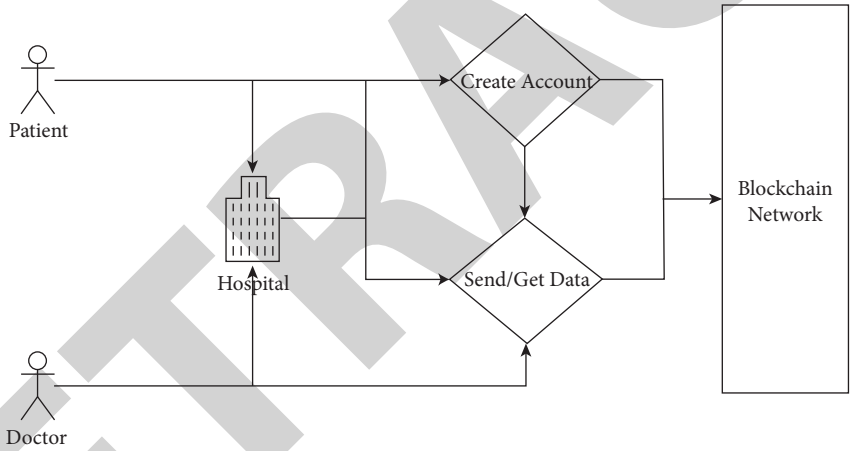

Figure 2: Process of system.

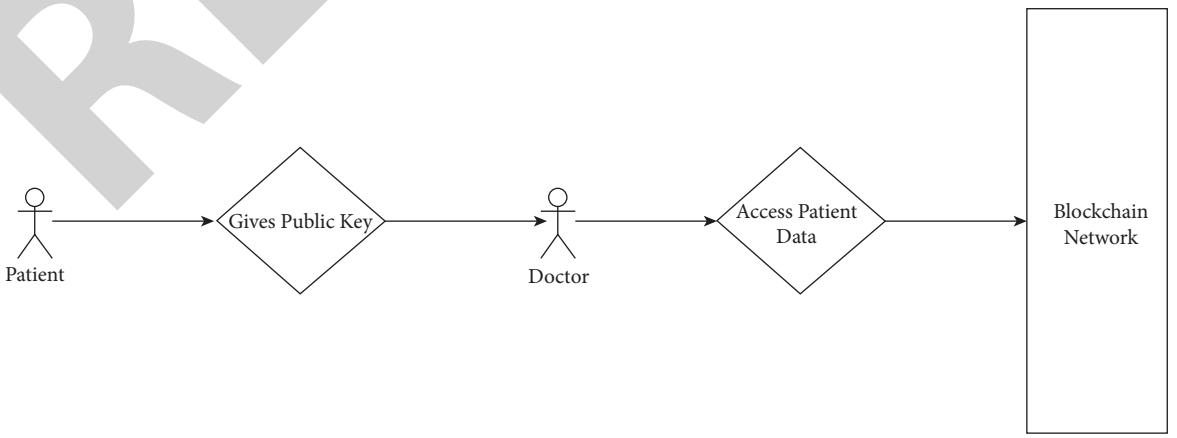

Figure 3: Authentication of public key and blockchain network.

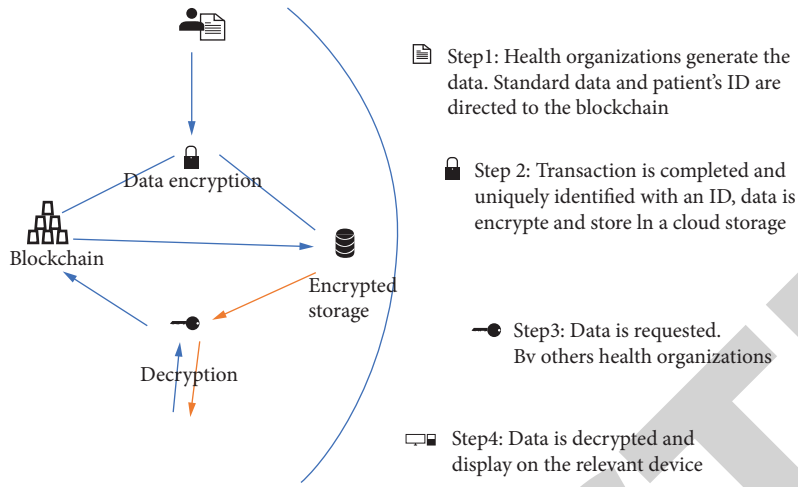

Figure 4: Blockchain data storage.

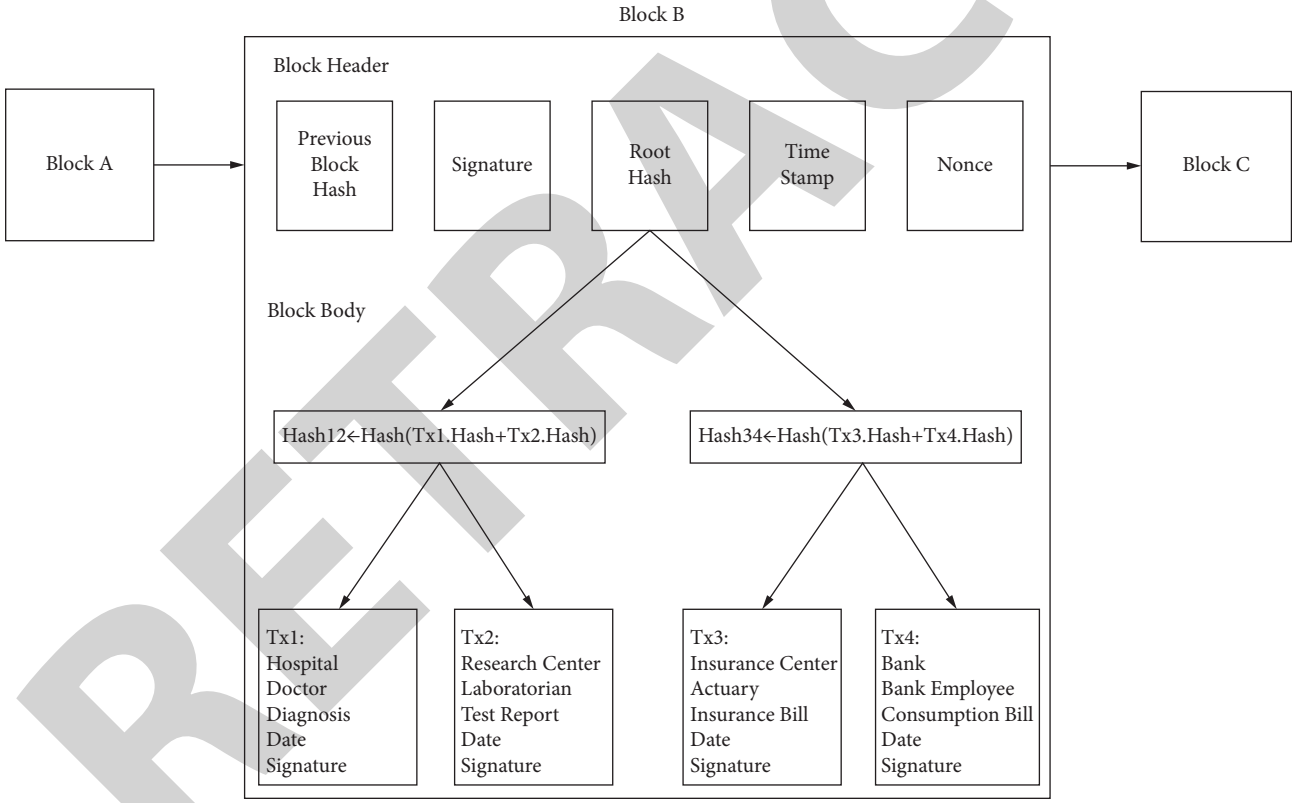

Figure 5: Block details in chain.

admin account, patient account, and doctor account are the three key aspects of this page. The username and private key will be required if the user already has an account. A private address is required if someone is creating one for the first time. Every action can be tracked and controlled. JavaScript, CSS, HTML, and Solidity were used to create this website system.

Figure 8 shows the signup page. Figure 8 shows how the data will be typed and stored in the local database once the user fills out the registration form with information such as their username and private address. The information may be viewed via the administrative control panel.

2.3. Data Security and Transaction in Blockchain and Smart Contract. Transactions do not appear in the block by accident. The list must be empty when one transaction occurs. Otherwise, it will not receive all of the individual data. Each block cannot contain the same data. If a majority of nodes agree on a transaction, it is included in a block. The

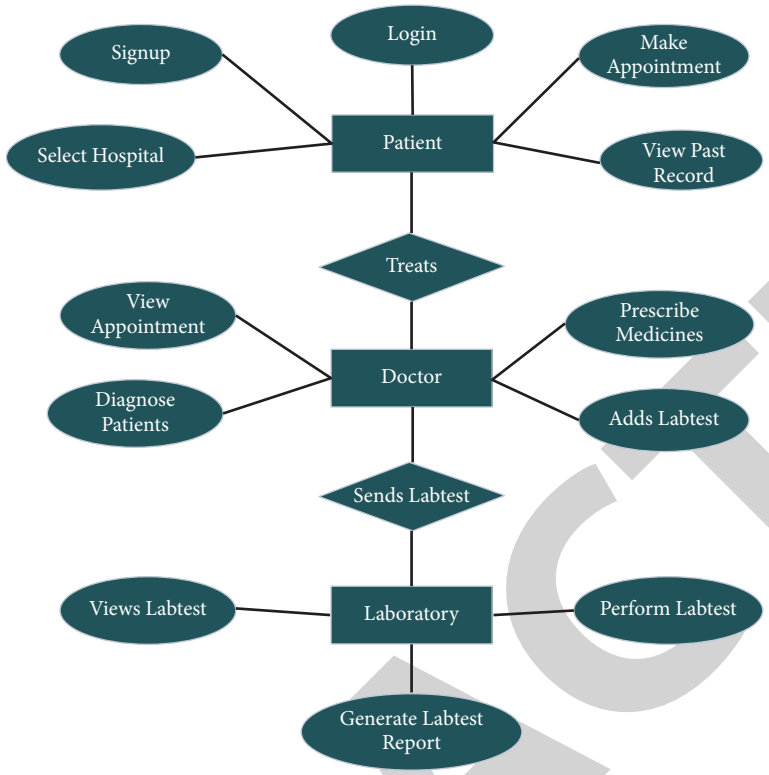

Figure 6: Entity relationship diagram of electronic health record (EHR).

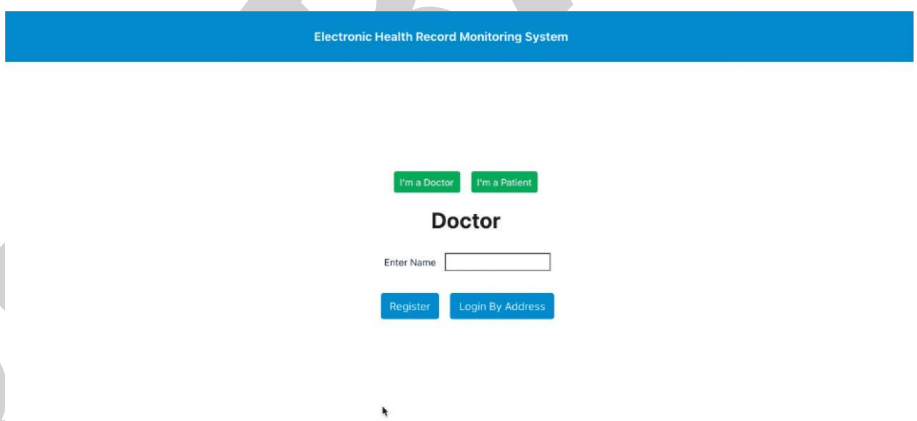

Figure 7: Login page.

blockchain is formed by each block referencing the previous block. A miner should verify whether a transaction fulfills the criteria to be processed before adding it to their block, depending on the blockchain's history. The transaction is genuine, according to blockchain history, and should be included in the block if the sender's wallet balance is sufficient. Privacy key by address is shown in Figure 9.

The data owner loses all rights to the deed if it is hacked or changed, as shown in Figure 9. It is a risky approach to possess something that may be deceptive at any moment. If only one line of data is deleted, the license for the data may be revoked. In conventional databases, client-server networks are utilized. A user (also known as a client) has the ability to make modifications to data stored on a central server. The database is still under the jurisdiction of a designated authority, which checks a client's credentials before allowing access. Because of database administration, if the authority's security is compromised, the data may be altered or even deleted. We can term blockchain technology an immutable ledger after using it here.

Figure 10 shows the immutable ledger with security. It is hard to alter the data if everyone retains all of the information in the block. Because all of the data in the block is linked to their prior hash number, if any of the data in the block is altered, the whole system is notified. It also has its own transaction mechanism that is very safe and reliable. These are

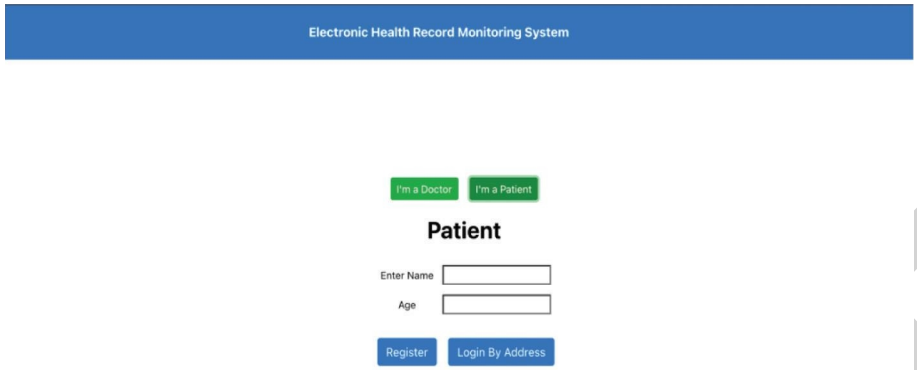

Figure 8: Sign-up page.

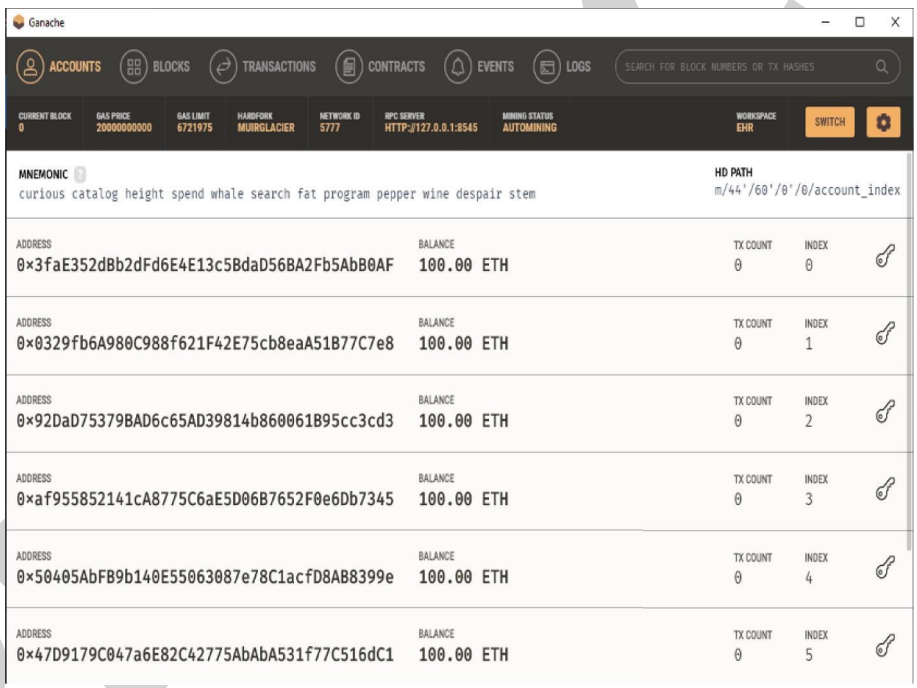

Figure 9: Private key by address.

the characteristics that distinguish any conventional ledger as immutable. A key characteristic of blockchain technology that distinguishes it from traditional database technology is public verifiability, which is achieved through integrity and transparency.

2.4. Chain and Data Component. This section explains the core notion of smart contracts by discussing the nature and types of contracts. We begin by defining the basic features of contracts and their many functions throughout the partnership's lifecycle from a legal and economic standpoint. Then, after looking at a few other definitions, we provide a general description of smart contracts. Last but not least, the importance of distributed ledger technology is discussed in the last part of this section. It displays all of the functions that were imported. When a block is produced and mined, the datetime function is used to give it its own timestamp. Because the function in disguise of a hash will be used, the function may need to hash the blocks in order for it to be effective.

Figure 11 shows us the JSON function. Before we hash the blocks, we will encode them. A class will be required. Because this will be performed through the use of a web application that will grab the message and utilize a postman to interact with the blockchain, a genesis block, a chain function, and a block function are all included in the blockchain class, and they are all responsible for adding and

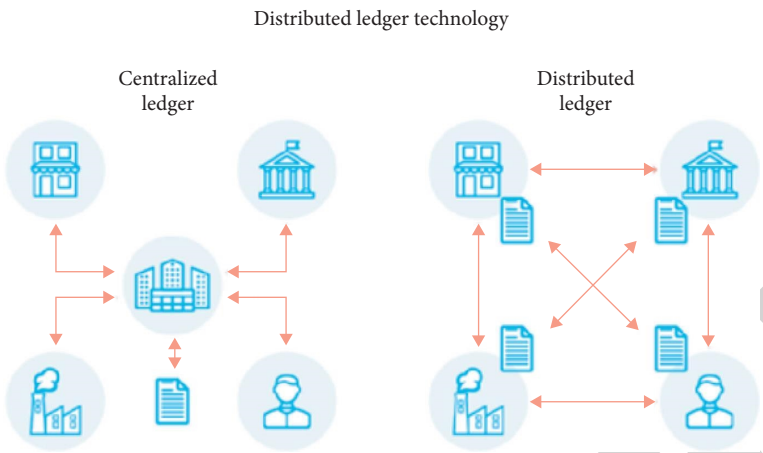

Figure 10: Immutable ledger with security.

```
function getFileInfo(bytes32 fileHashId) internal view checkFile(fileHashId) returns(filesInfo memory ) {
    return hashToFile[fileHashId];
}
```

Figure 11: Function for blockchain.

mining new blocks. The generate block function takes two arguments: a proof and the previous block's hash number. The function proof of function takes two parameters. The first is self, which is used to access a class-generated instance object. The second is an instance. In addition, there is the prior proof, which provides a path for miners to follow in order to solve the issue.

The function of file check is presented in Figure 12. Figure 12 illustrates that the new proof value is 1, indicating that after each repetition, the value of the proof must be increased by one until the correct evidence is obtained. Check proof will do the necessary checks to determine if the proof is valid or not. In addition to having four leading zeros, which makes mining for the hash operation more difficult for miners, the hash operation is made up of a string of 64 characters. The encode function will encode the string in the correct format, which is the format that the sha256 function expects to be sent. In this transaction, the transaction's function has been defined. With the help of the self, sender, and recipient keys in the argument, this add transaction method will carry out the procedure. This will complete the transaction before it is included in the block of transactions. The append method will be used to add a new transaction to the end of this collection of data. It is necessary to include the prior data for each new transaction, and this will be accomplished via the previous block function in each transaction. It will add +1 to the previous block function before returning to the previous block function. As a result, the number will automatically rise, the list will grow, and the information will be preserved.

2.5. Transaction Component

2.5.1. Encryption Methodology. In a blockchain, all the information provided by a doctor or patient is encrypted using cryptographic functions. In this research work, we have used the "keccak256" function built into Solidity. As shown in Figure 13, this function takes an input and converts it into a hash with a fixed length of 256, making the data provided by patients and doctors highly confidential.

Figure 14 shows the output of the keccak256 function. What is important here is that whenever a slight change is made to the string, the hashed output changes drastically. A blockchain is formed only when each of the blocks is referenced by one another. Each block has the data and a hash pointing at the next block in the blockchain. This makes our system highly secure as even the slightest tampering with the input data will change the hashed output. Then, it will also change the hash of the previous block and the one before it, and subsequently, the whole blockchain will break. When this code is run using the keccak256 function, the string "ABC" gets converted into a hashed output.

2.5.2. Smart Contracts. Figure 15 shows the smart contract example and transactions. According to Figure 15, it is observed that smart contracts are deployed to facilitate, verify, or enforce negotiation of digital transactions. It separates the negotiating parties from any third party. Smart contracts are basically pieces of code that are programmed to verify certain conditions. If those conditions are not met,

```
function getFileSecret(bytes32 fileHashId, string memory role, address id, address pat) public view
checkFile(fileHashId) checkFileAccess(role, id, fileHashId, pat)
returns(string memory) {
    filesInfo memory f = getFileInfo(fileHashId);
    return (f.file_secret);
}
```

Figure 12: Function of file check.

```
pragma solidity ^0.5.0;

contract Test {
   function callKeccak256() public pure returns(bytes32 result){
      return keccak256("ABC");
   }
}
```

Figure 13: The keccak256 function converting a string.

```
0: bytes32: result 0xe1629b9dda060bb30c7908346f6af189c16773fa148d3366701fbaa35d54f3c8
```

Figure 14: The output of the keccak256 function.

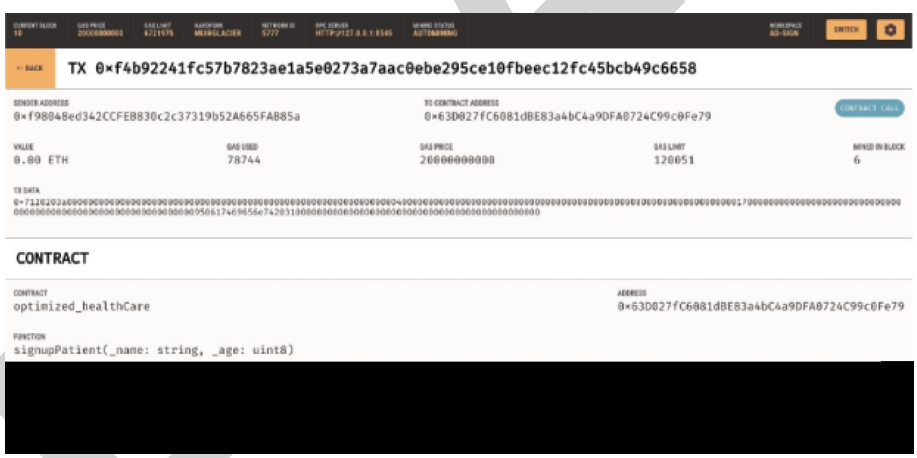

Figure 15: Smart contract example and transactions.

then the transaction will not happen. We have programmed many smart contracts throughout the system and those smart contracts only execute when the conditions are met.

2.5.3. Mapping and Modifiers. A mapping function example is shown in Figure 16. Mapping is a function in solidity that exists in a key-variable relationship. It takes a key and returns a variable. An access modifier can be set on the returning variable. The address is the unique public key half of the Ethereum address of the interacting party. In the first mapping of Figure 16, the mapping function takes the address of the interacting party and then returns the list of doctors and list of patient profiles he can access. Since the access modifier is private, nobody outside the contract can view this information. The modifiers are used to check if that doctor exists or not, which is shown in Figure 16.

Figure 17 shows a modifier example. Figure 17 demonstrates that a large number of very strong security measures have been applied, resulting in a system that is exceptionally secure and dependable. As a consequence of their failure to address these concerns, other publishers' systems have become insecure and susceptible to hacker attacks. It satisfies the standards since it features an immutable ledger, smart contracts, blockchain-compatible transactions, and straightforward refund and return mechanisms. Almost every argument offered in earlier articles contains a fault. The inability of some of the website's administrators to correctly execute the smart contract was the primary cause of the website's collapse.

```
mapping (address => patient) private patients;
mapping (address => mapping (address => uint)) private patientToDoctor;
```

Figure 16: Mapping function example.

```
modifier checkDoctor(address id)
  doctor memory d = doctors[id];
```

Figure 17: Modifier example.

3. Result and Comparison Analysis

We have developed an EHR system for Bangladesh. Actually, in South Asia, EHR is much less than in North America. The main reason is the Blockchain ecosystem and structure. The study summarizes initiatives throughout Asia to deploy EHR systems for a variety of purposes. We highlight 32 pieces of research performed in 15 countries, including two that compare locations throughout Asia. This study collects data on EHR systems in a variety of countries and healthcare situations, including LMIC settings, diverse organizational structures, and various levels within health systems. It reflects a range of technical infrastructure and EHR system "maturity" levels, as well as the resulting human resource requirements.

This research analyzes the obstacles to the use of electronic health record systems in developing healthcare in subcontinental countries. Restrictions on the framework needed for EHR systems (e.g., stable electricity, wireless technology, and other mobile technologies) add another degree of complexity to system requirements and the level of EHR sophistication that may be supplied. As a result, there may be risks associated with using EHR for public health purposes in a particular context. Several of the most important hurdles are connected to organizational culture, and they underscore the crucial necessity for well-trained technical assistance in Asian hospital environments. Hospitals often discover that delays in EHR deployment arise as a result of physician and health professional nonadoption of the system. According to research conducted in Iran, organizational obstacles to EHR adoption include a lack of effective planning, a shortage of qualified personnel, and restrictions on healthcare workers' access to information technology training. In light of these concerns, potential solutions include conducting a priori assessments of organizational cultures and settings where EHR systems will be implemented in order to determine the level of technical support required; examining staff understanding, experience levels, and readiness for new software; and reviewing current data harvesting systems in order to minimize early deployment bottlenecks. In addition, before a system is implemented, it is important to address staff concerns about new information and communications technology interventions. This will help to prevent reluctance to adopt new practices and alleviate concerns about the administration of the burden associated with the new system. Implementation within a specific health system or organization may benefit from these investigations because they allow for a more customized approach to EHR interventions that are contextualized in light of unique externalities that may present obstacles but cannot be addressed at the implementation level. In addition to technological and practical challenges, research has shown that the adoption of EHR therapies is fraught with ethical concerns. As electronic health records (EHRs) become more common in low- and middle-income countries (LMICs), continuing concerns in HIC about patient confidentiality, privacy, informed consent, and data security continue to be important in resource-constrained settings. Aside from highlighting the reality that worldwide EHR systems are increasing at a rapid speed, it also highlights the problem that LMIC settings may be underprepared to deal with the difficulties connected with EHR adoption. Many smaller healthcare providers and independent hospitals are still looking for successful EHR systems, or are transitioning from fragmented applications provided by a variety of suppliers to a single, functional system. It is necessary to carefully consider patient-provider interactions in low- and middle-income countries (LMICs). These interactions must take into account cultural sensitivity, ethnic health inequalities, low levels of patient literacy, language difficulties, and the need for institutional supervision of the patient-provider connection. To ensure that efficient and flexible EHR systems are deployed to meet public health needs in the future, more systematic and comprehensive preparations should be undertaken. In the same way that technical and practical barriers must be overcome when implementing EHR interventions, ethical issues must be addressed in order for effective EHR initiatives to be implemented successfully. It is anticipated that by developing a framework for EHR implementation and providing formal instruction to healthcare professionals and support personnel on ethical issues, healthcare providers and support staff would be able to minimize patient risks. Because we did not have access to any computer calculations, we

Table 1: Comparison with other papers.

Point of this paper	Point of other papers
(1) Medical data is encrypted from end to end by the user. No third party can see the details.	(1) The data received from the end user is first encrypted so that it is only visible to them [1].
(2) We used cryptocurrency transactions. It will be revolutionary.	(2) No cryptocurrency transactions [21].
(3) We have used the "keccak256" function built into Solidity. This function takes an input and converts it into a hash with a fixed length of 256, making the data provided by patients and doctors highly confidential.	(3) Authors discussed about many variations of EHR's security [9].
(4) Patients and doctors will both benefit. Every service under our system will be faster than under the current system.	(4) Some EHR systems need more time to update the information. Sometimes, the system needs more electricity to run the server. It is expensive [20].
(5) We have used secured databases to monitor every footprint on the web. It will be stored on the server in a hash. So, no one can temper the medical data easily. It Is under smart contracts.	(5) The system is controlled by the admin. Sometimes, records cannot be undone. So, its footprint is so strong that it finds the bad side of the system [7].

Table 2: EHR lifecycle factors.

EHR lifecycle factor	Usability and safety optimization opportunities	
	For EHR developers	For healthcare providers
Safety	• Incorporate a safety practice into the organization's policies so that all team members understand its value. • Create a risk-free atmosphere in which possible risks may be reported. • To classify and act on discovered issues, use a specialized professional with expertise in patient safety and risk management. • Consider security measures in current and prospective software versions. • Allow workers and customers to report safety risks and communicate promptly about the stated danger.	• Set up a safe space where employees may come forward with concerns about potential dangers. • Prioritize safety by implementing measures to make sure that everybody on the team understands how important it is. • Authorize the use of automatic surveillance to look for potential risks in case of setup errors. • Use teams with embedded health IT knowledge, especially in big companies with internal specialists in health information technology (health IT).
Product R&D	• Develop and improve infrastructure by identifying healthcare provider requirements. • Find out what kind of training you need. • Prior to the introduction of a product, carry out testing that focuses on high-risk functionalities and involves targeted users who are representative of the target market and rigorous test scenarios.	• Provide developer employees with chances to study healthcare staff processes and technology usage. • Design and testing for usability and safety should be shaped by physicians and experts in the field.
Acquisition	• Provide healthcare providers with upfront information about the HER product's features and anticipated prices so that they may examine the product's viability, such as through comprehensive documentation.	• In order to identify prospective suppliers, evaluate clinician requirements for the EHR product as well as any budgetary restrictions.
Customization and configuration	• Create a list of known high-risk modifications that defy developer advice and explain how and why they may affect patients. • Clarify with providers the relevant definitions, resources, and responsibilities (vendor, provider, and third-party products) • Analyze the resources and expertise of the supplier to make adjustments to the product and interact with them.	• Evaluate internal capabilities and expertise to modify the product based on talks with the vendor. • Create a compelling argument for why modifications are necessary, including use cases. • Document customizations that are made and develop a risk mitigation plan.

Table 2: Continued.

EHR lifecycle factor	Usability and safety optimization opportunities	
	For EHR developers	For healthcare providers
Implementation and upgrades	• Create an implementation strategy based on your knowledge and share it with the teams in charge of implementing it at the healthcare providers. • Help implementation teams at healthcare facilities, such as doctors and nurses, and understand the fundamental functions and processes. • Ensure that a mechanism is in place to monitor safety by encouraging facilities to review their risk management procedures, resources, and requirements. • A well-qualified and well-supported IT staff is essential for providing on-going assistance.	• Implementation procedures must be supported by a sound governance framework that addresses any safety concerns that may emerge. • Set up implementation teams of experts from various fields who can come to an agreement on the functionality and process. • Select a representative group of users to evaluate the new product. • As soon as new versions of your operating system are available, begin implementing them. • Identify areas that need further construction, configuration, and/or clinical risk analysis and mitigation by reviewing changes included with updates.
Training	• Incorporate training situations that are both demanding and safety-focused. • Refresher training should be provided following any significant system modifications or upgrades. • Train your employees with the help of professionals who are trained or certified in the new technology you have bought.	• Keep track of the training expenses and the steps you took to get there. • Personalized training that meets the specific requirements of the participants is essential. Workflow simulations, refresher training, ongoing access to training materials, and the chance for improved training for individuals in need are all ways to provide this kind of training. • Learn to take into account the finest training methods suggested by vendors.

came up with a list of advantages and disadvantages of how the system would affect the lives of healthcare and information technology professionals.

The points of this paper are compared to the points of other studies in Table 1. The facts concerning EHR are presented in this article.

Table 2 shows the analytical points that if we implement EHR, the healthcare providers will benefit and how all the structures will be organized in detail.

4. Conclusion

The purpose of this article is to improve the intelligence and security of electronic health management. This architecture is unchangeable and provides complete transaction transparency. It guards against unwanted access and data tampering on our website. Smart contracts also reduce the amount of time spent on time-consuming documentation. In general, medial data administration entails a great deal of paperwork. Smart contracts are immutable because of the blockchain, which saves the information as evidence. This paradigm has the greatest impact on transactions, immutability, and refundable procedures in chain management. An end-to-end approach was suggested in this research. The function and role of each actor have been defined. It also implies that our framework may be used in a wide range of situations. In addition, the construction of smart contracts is explored. As a consequence of the results of this article, the problems that people have with outdated processes will be permanently removed. This study creates trust to develop and reduce transaction costs, as well as improve financial inclusion by providing additional options for those who do not have easy access to financial services, among its many advantages (the most significant of which is the ability to keep data secure). This is a small-scale, one-of-a-kind piece of work. The delay may be impacted if there is a high amount of data. In terms of storage and processing expenses, blockchain transactions will be very advantageous. Another approach to increase performance is to use decentralized databases. Furthermore, tracking devices may be added to the structure in the case of a large-scale deployment. As the amount of data grows, we may employ off-chain architecture to store the original data, with the proof of existence remaining on the blockchain. This may be a possible study subject for this inquiry in the future.

Data Availability

No data were utilized to support these research findings.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

The authors are thankful for the support from Taif University Researchers Supporting Project (TURSP-2020/115), Taif University, Taif, Saudi Arabia.

References

[1] A. Bakhtawar, R. J. Abdul, C. Chinmay, N. Jamel, R. Saira, and R. Muhammad, "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic," *Personal and Ubiquitous Computing*, vol. 1-17, 2021.

[2] C. Chakraborty, *Mobile health (M-Health) for tele-wound monitoring. In: Mobile Health Applications for Quality Healthcare Delivery*, IGI Global, Hershey, PA, USA, pp. 98–116, 2019.

[3] C. Chinmay, B. Gupta, and S. K. Ghosh, "A review on telemedicine-based WBAN framework for patient monitoring," *Int. Journal of Telemedicine and e-Health, Mary Ann Libert inc.*vol. 19, no. 8, pp. 619–626, 2013.

[4] Y. Shelke and C. Chakraborty, "Augmented reality and virtual reality transforming spinal imaging landscape: a feasibility study," *IEEE Computer Graphics and Applications*, vol. 41, no. 3, pp. 124–138, 2021.

[5] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, Montreal, QC, Canada, October 2017.

[6] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: a block Architecture," *IEEE Access*, vol. 6, Article ID 32700, 2018.

[7] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[8] L. Ismail, H. Hameed, M. Alshamsi, and M. Alhammadi, "Towards a blockchain deployment at UAE university: performance evaluation and blockchain taxonomy," in *Proceedings of the 2019 International Conference on Blockchain Technology*, pp. 30–38, Honolulu, HI, USA, July 2019.

[9] A. Juneja and M. Marefat, "Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification," in *Proceedings of the 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)*, pp. 393–397, Las Vegas, NV, USA, March 2018.

[10] E. W. Jamoon, N. Yang, and E. Hing, "Adoption of certified electronic health record systems and electronic information sharing in physician offices," *NCHS Data Brief*, vol. 236, 2016.

[11] E. Kim, S. M. Rubinstein, K. T. Nead, A. P. Wojcieszynski, P. E. Gabriel, and J. L. Warner, "The evolving use of electronic health records (EHR) for research," *Seminars in Radiation Oncology*, vol. 29, no. 4, pp. 354–361, 2019.

[12] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 130, 2018.

[13] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: a systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541–562, 2013.

[14] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, p. 136, 2018.

[15] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, pp. 5–17, 2018.

[16] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics Journal*, vol. 25, no. 4, pp. 1398–1411, 2019.

[17] European Parliament, "Council of the European union directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

[18] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, pp. 1–11, 2019.

[19] HHS.Gov, "The HIPAA privacy rule," 2000, https://Electronic.hhs.gov/hipaa/for-professionals/privacy/index.html.

[20] S. Nakamoto, "A peer-to-peer electronic cash system," 2008, https://bitcoin.org/bitcoin.pdf.

[21] Who Owns Medical Records, "50 state comparison," 2021, http://Electronic.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison.

[22] P. H. R. Mtbc, "Personal Health Records for Patients," 2021, https://phr.mtbc.com/phrdefault.aspx.

[23] P. H. R. Capzule, "Your family health data in one app," 2021, https://Electronic.capzule.com/.

[24] GenexEHR, "Individual electronic health record-GenexEHR," 2014, https://Electronic.genexehr.com/individual-electronic-healthrecord.

[25] M. D. Turjo, M. M. Khan, M. Kaur, and A. Zaguia, "Smart supply chain management using the blockchain and smart contract," *Scientific Programming*, vol. 2021, Article ID 6092792, 12 pages, 2021.