Protect medical records by using blockchain technology

Marwa Sami Mohammed, Asaad Noori Hashim
Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

Article Info

Article history:

Received Apr 18, 2023
Revised Jun 10, 2023
Accepted Jun 17, 2023

Keywords:

Blockchain technology
Ethereum
Inter planetary file system
Medical record
Smart contract

ABSTRACT

Recently, medical records have been stored and shared locally, which creates a risk of data loss or corruption; these records may be stored and shared through cloud-based central data centers; nonetheless, this strategy has disadvantages, such as the need for significant storage space and the privacy concerns associated with network-wide data sharing. Medical records require increased security and confidentiality, furthermore, these records must be protected when transmitted to and shared with doctors of the same specialization, to solve this problem, blockchain technology was used as a decentralized technology that offers a secure and immutable way to store and protect information. In this paper, a website is designed that uses blockchain technology to save medical records and employs smart contract technology in the ethereum blockchain to govern the creation and display of files and sharing. An interplanetary file system was used to offer a mechanism for the decentralized storage of medical images and reports while maintaining their accessibility on a global scale, it is available only for doctors who have the authority to access them, and the proposed system proved efficient in saving and sharing medical records with high security and less cost.

Corresponding Author:

Marwa Sami Mohammed
Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa
Najaf, Iraq
Email: marwa.mawash@student.uokufa.edu.iq

1. INTRODUCTION

Healthcare advances that include patients' DNA, lifestyle, and environment have expanded tremendously, these advance has increased healthcare participation, databases, and data tracking systems, these healthcare and IT innovations would change health IT [1]. Medical images provide almost 70% of diagnostic data essential for disease diagnosis. However, more than 90% of medical facilities experience patient data breaches, so protecting it is critica [2]. Academics in healthcare have sought a practical means to store and distribute medical data and images, cloud-based, centralized information centers curently in use require additional storage and upkeep and have privacy issues regarding network data sharing. Hence, large health records must be transferred and stored securely [3].

Blockchain technology can protect a patient's medical records and alleviate health IT interoperability challenges by securely exchanging individual, provider, and research-level electronic health records [1], [4], so it can substantially assist healthcare, and that is through giving a model that focuses on the patient in the first place and gives priority to the available resources and adequate services [5], as well as blockchain can be used to secure sensitive patient data and regulate access to it, providing a safe place to store it and an efficient way to access it [6]. The blockchain is a series of blocks containing information; these blocks are connected using a cryptographic procedure called a hashing function, when these blocks are linked together, an unbreakable chain results [7], [8]. Blockchain nodes compete and collaborate to maintain a precise ledger, blockchain technology is a fast-growing security cryptography system with decentralized solutions outperforming many security techniques; data in it is unchangeable, it is characterized by Immutability, which means safety, security, strength, and resistance [9], [10]. Blockchain storage is restricted and difficult for storing images and medical data, as a result, protocol labs built a decentralized storage web called interplanetary file system (IPFS), IPFS enables the storage and distribution of hypermedia through content-addressable P2P protocols. IPFS and other blockchain networks are compatible thanks to off-chain storage because the IPFS hash functions have significantly reduced the amount of blockchain data [3], [11]. Systems for distributed data access become quicker, wiser, and more durable thanks to IPFS [3]. IPFS is a large-scale peer-to-peer (P2P) distributed system that uses lib p2p to establish a network of computers linked by a common storage medium [12], combining blockchain and IPFS improves application speed and throughput through memory optimization and decreases transaction latency [13]. Multiple blockchain platforms have appeared one of them ethereum is a distributed ledger platform that features smart contracts, it is open source and anybody may create secure apps on it [14], [15], ether is a network-dedicated encrypted currency that facilitates peer-to-peer contracts [15].

The ethereum virtual machine (EVM) lies at the heart of this platform, allowing it to execute sophisticated algorithms, decentralized applications (DApps) use a contract-oriented programming language for their code solidity programming language [16], this platform supports the term smart contracts are digital transactions that automatically carry out the terms of contracts [17], capable of performing simple functions when programmed [18], smart contracts are tested in a platform called remix is an open-source application that permit users to write code in programming language solidity, JavaScript was utilized in the development of remix, and it may be used both locally and in the browser, as well as provide testing, debugging, and deployment of smart contract [9]. It is often used with a blockchain wallet to pay fees, metamask is an addition for browsers that enables users to access and interact with the dispenser web within the browser. It makes it possible to execute decentralized apps built on ethereum directly in the browser [19], metamask is a web browser that enables the execution of ethereum DApps without installing and maintaining a complete ethereum node. It also includes a wallet for safe identity, managing online identities and signing blockchain transactions [20].

Currently, web applications are increasingly prevalent across various internet-based services, security is a significant consideration for applications, a significant number of web applications are susceptible to vulnerabilities, rendering them appealing targets for security attacks [21]. Consequently, the use of blockchain technology with web applications is also beneficial of the data stored by these websites. Many researchers have discussed the importance of blockchain in protecting medical data and the medical system.

Xia *et al.* [22] present a MeDShare, a blockchain-based technology that checks and regulates shared medical data in cloud repositories. It ensures the integrity of all data transfers and sharing between entities and all system functions. It uses smart contracts and an access control mechanism to track activity and remove access to organizations that breach data permissions. MeDShare works just as well as other cutting-edge technologies for sharing data between cloud service providers without putting data privacy at risk [22].

Fan *et al.* [23] presented the idea of using a blockchain-based information management system called MedBlock to deal with patient records. MedBlock’s distributed ledger facilitates quick and easy EMR access and retrieval in this setup. The enhanced consensus technique allows EMR consensus to be reached without excessive energy use or network bottlenecks. Due to its symmetric encryption and individualized access control algorithms, MedBlock also displays a high level of data security. When sharing private medical data, MedBlock may be an invaluable tool.

Shen *et al.* [24] proposed a MedChain is an effective approach for distributing healthcare data that blends structured P2P networks, digest chains, and blockchain technology, a session-based healthcare data-sharing system has been created that is based on MedChain and offers greater data-sharing flexibility. The study’s conclusions show that MedChain can increase efficiency and adhere to data exchange security criteria. Patel [25]. proposed a system for sharing images across domains that uses blockchain as a distributed data storage to create a ledger of radiological exams and patient-defined access rights. It is shown that the Blockchain framework stops third parties from getting access to protected health information, meets several standards for interoperable health systems, and is easy to use for things other than medical imaging. The architecture has some flaws, such as privacy and security models that are hard to understand and a regulatory environment that is hard to understand.

Muradova and Hematyar [6]. the author suggested that blockchain technology might be used in E-health to preserve, protect, and anonymize data. Showed how blockchain-based medical records might improve diagnosis and treatment in a secure, fast, decentralized manner. This research involves the process of protecting, securing, and creating the medical blockchain.

Jabarulla and Lee [3] patient-centric image management (PCIM) is a system that uses the ethereum platform in blockchain and the interplanetary file system to store and send medical pictures without a central server IPFS, as an alternative to the present access management system. A patient-centric access control protocol based on a smart contract was established, which provides privacy, safety, access adaptability, and expenses. It keeps and provides access to medical photos within an open distributed network while giving patients total ownership of their images and complete transparency, smart contracts were also employed to offer patient-centric access management, allowing individuals to give or cancel access to their provider [3].

Haleem *et al.* [5] the researcher discusses blockchain technology and its most important uses in the medical field, with the goal of; i) figuring out the "unified work-flow process" of putting blockchain technology to use in healthcare and ii) talking about how blockchain technology can help improve healthcare services. Mhamdi *et al.* [26] this study introduced secure electronic medical record (SEMRAchain), an access control (role-based access control) (RBAC), attribute-based access control (ABAC), and smart contract (Sc)-based system. This integration allows the decentralized, granular, and dynamic administration of EMR access control, by combining the features of a distributed ledger with authorization mechanisms, this assurance is provided by blockchain technology to all parties involved in the system, and multiple smart contracts for access control are available. This smart contracts validate access requests, check policies, and check misbehavior, calculating smart contract and function costs evaluates the proposed system.

The submitted paper presents a solution for a protected medical record (PMR) system that ensures patients are safe and keep track of their private information without using a central infrastructure. A website was created to store and distribute medical files and images. A patient-centred access control protocol using ethereum SC was created to provide a decentralized and reliable access control policy. IPFS was used to facilitate the decentralized storage and worldwide accessibility of medical images and content. Many people who logged in via the metamask wallet tried a prototype of the system, and images and files were uploaded to the system and created records, and those who could view the specified record were controlled. The subsequent sections of this paper are arranged in the following manner: the second section of the paper describes the proposed method, and in the third section, the designed system, its components, and the algorithms used in the proposed system are explained. The fourth section explains the practical results of the system. And prove the efficiency of the proposed system, we conclude this paper in the fifth section, which discusses this paper briefly, the efficiency of the proposed system, and the results obtained.

2. PURPOSE METHOD

The proposed system is a website used to store and share medical records confidentially and safely and to allow doctors licensed by the doctor who created the record to view the specific patient's record, the created record contains medical images and a PDF file containing patient reports, information about him, and his current diagnosis. The proposed system firstly created using the ethereum blockchain technology, the smart contract feature in ethereum was used to set the necessary conditions for creating the record, the main condition here is that the record must be created by the owner only, and the owner here means the person who logged into the wallet. The second condition is that it only must display the specific records of people licensed by the doctor who created the record, and they are in aspecial list, the records within the site are of two types, records created by the owner doctor who logged in and records that shared with him by other doctors. Inter planetary file system file system was used to store images and medical files by registering on infura. This site provides you with a link that is added to to the hash value coming from the IPFS to enable the display of images and files. The metamask wallet is used for logging in to the site to create and view the records the Figure 1 is shown the proposed system.

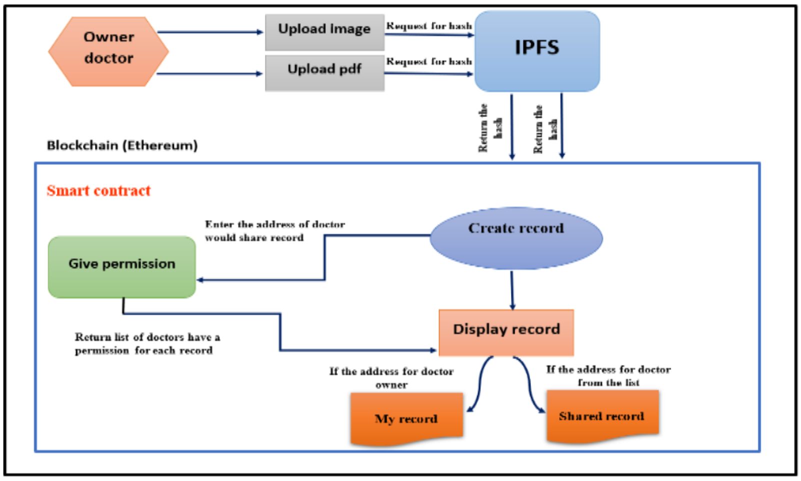


Figure 1. The proposed system

3. METHOD

As previously mentioned, PMR model is a website, and to design any website, we will need three main components: the front end, which is what users see and intract with it to be able using the proposed system; the back end, which is the invisible structure that makes the front end executable, and the link between the front end and the background which iclude all linking requirment to to achieve integration for system. Figure 2 shows the structure of the proposed system and its components mentioned previously.

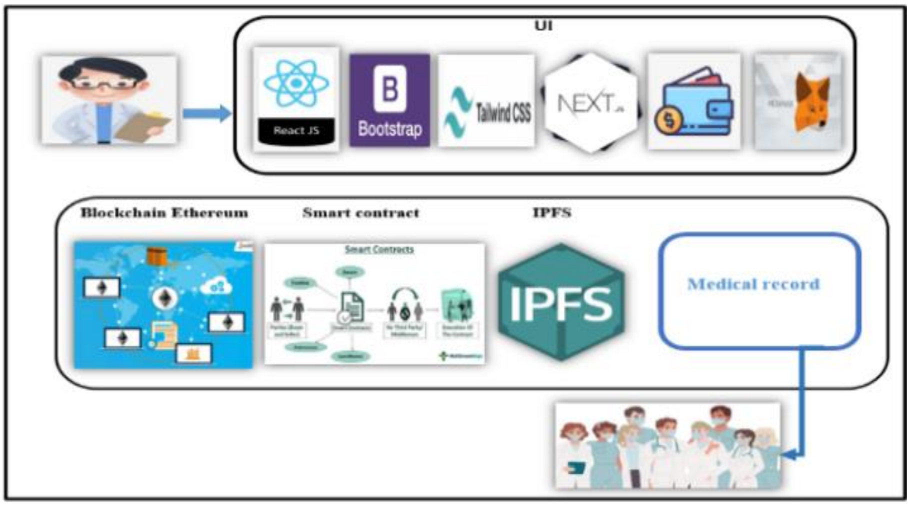


Figure 2. PMR model

3.1. Frontend

The frontend refers to everything the user sees and interacts with on a website, including the navigation bar, the menus, and the contact form. Tools and libraries like hypertext markup language (HTML), cascading style sheets (CSS), and JavaScript, managed by the browser, are used to create and build a frontend web interface [27], in the front end part, a project was made to design the user interface (UI) and the hardhat project, which will connect the front end to the back end later. The UI was designed using JavaScript, which enabled it to be used as a programming language on the server side. Node.js was installed, and the node.js package manager was included to help developers deal with software in an environment of node.js, many libraries for the JavaScript language were used in the proposed system.

React.js is a library of the JavaScript language used to build user interfaces, and it is an open-source library, the interactive interfaces of the site were created using this library after designing the initial interfaces in the Adobe XD program, it is the portal that enables the user to interact with ethereum blockchain. React redux is considered an official link to the user interface, constantly updated with any changes in the API, they were used in the proposed system to ensure that the react components work as expected, in addition, they help maintain data after the wallet is disconnected, that is, when exiting from the site. The next.js library is also used in UI design, it is also considered an open-source library for react and is lightweight, making it easier for developers to create static applications, it is also considered as react framework, it was used in the design of the site because it shortens the use of many other libraries. this library was used in designing the project pages, such as the index.jsc, document.jsc, about.jsc, connect.jsc, contact.jsc, creat-record.jsc, app.jsc, as well as it helps to make a special uniform resource locators (URL) for each page on the site; it is also responsible for navigating between project pages. The other important library used in designing the site interface is tailwind CSS, it is responsible for the style in CSS, it works by scanning all files of HTML and components of JavaScript and any other templates for class names and creating the corresponding styles. Then writing them in a static CSS file, it was used on the site to design a look, buttons, colors, writing methods, this library is fast, flexible and reliable. Bootstrap was also used, which is considered a free and open source framework used in designing websites and web applications because it contains ready-made templates, classes written in CSS and JavaScript, and HTML, and it is considered the most used environment in front end design because it is compatible with all screen sizes. It was used in designing buttons and boxes, text, dropdown lists, and theme builders. The Figure 3 shows the libraries used to design the PMR model's user interface. The other part of the front end is the metamask wallet that we will install and create an account to log in to the site PMR model. Figure 4 shows the metamask wallet.

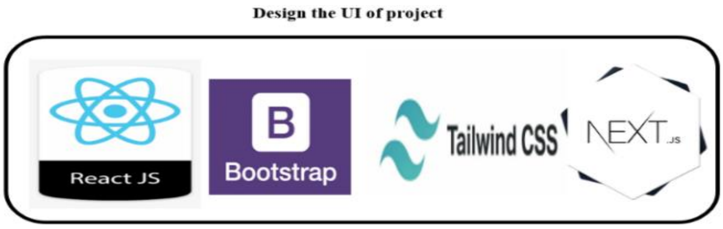


Figure 3. UI of PMR model

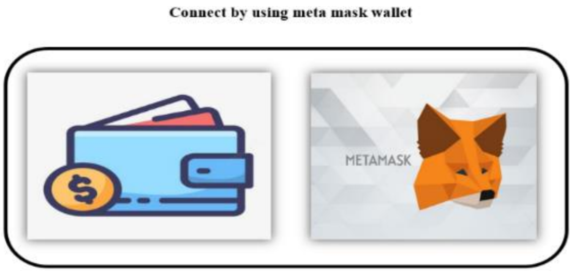


Figure 4. Metamask wallet

3.2. Backend

The backend typically includes a server, an application, and a database. These three components make up the backend. Backend technologies often include programming languages such as PHP, Ruby, and Python [22]. In the design of the medical records protection site, the backend represents the ethereum blockchain, which is the stage of writing the smart contract (SC) in the solidity language. A visual code environment was used to write the contract functions in the solidity language. The contract includes a set of important functions, and each will achieve a specific function in the proposed system.

The first function used for creating a record, this function requires several inputs, including the name of the image, the URL that includes the hash of the image and this URL that we get after storing the image in IPFS, the URL of the file, which is in pdf format, and it also includes the hash value returned from IPFS. After that, the record is stored in a list of records, including the address of the doctor who created the record, which is the same as the address of the metamask wallet that login by it. This function is explained in detail in the Algorithm 1.

Algorithm 1. Create record

```
Input:-image file, pdf file
Output:-record of [image, pdf]
*Initialize the record count
Record count < ---- 0
Begin
Step 1: - defining structure of record using struct types
        Struct record < ---- id, name, image file, pdf file, payable owner, [] doctors.
Step 2: - create mapping for list of records
        Mapping (=> record) private   list of records
Step 3: - checking the name, image file, pdf file: -
        3.1 if(name!=[])                            %not empty
                Require< ---- name. Length >0
        Else
                Print ("your name is empty")
        3.2 check the image file and pdf file if empty
Require< ---- (image file). Length && (pdf file). length >0
Else
Print ("your image file is empty")
Step 4: - Increment count of records
Records count< ----- ++
Step 5: - save records of each doctor
Doctors < ----list of records [count]. doctors
Doctors. push (address ()).
Step 6: - save the new record to the list of records
List of records < ------- record (count, name, image file, pdf file, payable (msg. sender),
doctors)
End.
```

The second is record accessible:-it is a function for displaying a specific record and its contained, a modifier was utilized, it was previously created to give the permission to the owner doctor of origin and the doctor who is on the list of doctors who have the license from the doctor who created the record, all they have been verified. This function is explained in the Algorithm 2.

Algorithm 2. Record accessible

```
Input:-The id of record
Output:-Information of record
Begin
Step 1: - defining structure of record using struct types include the id to define the
record
Struct record < ---- id, name, image file, pdf file, payable owner, [] doctors.
Step 2: - create a function (address array item exist) to check the address given is for a
doctor in the list of doctors have a permission
Begin
For each address in the list
If user address = = list of address
Return true
Else
Return false
Step 3: - create mapping for list of records
Mapping (=> record) private   list of records
Step 4: - using modifier for verification that the address is for owner or for doctor have
the permission to show the record
If address of array (msg. sender) list of record [id]. doctor) = = true || msg. sender = =
list of records[id]. owner)
Step 5: - view the record
Step 6: - return list of record
End
```

The third add permission: -the third function is giving a license to a doctor, in this function, we use modifier to anssure us that only the doctor who access the record can grant a license to another doctor to be able to view this record. In this function, we make sure that the address is not fictitious and that it is the address of the owner's doctor by comparing it with the address of the sending doctor, if it is equal, then he is the owner doctor, and he has the right to add the address of the other doctor to the list of addresses of doctors authorized to display this record.

The fourth records created by owner:-the fourth function is a function that displays only the records created by the owner doctor,in this function, we call all the records and use a counter to represent the total number of records and another counter to calculate only the records created by the owner, the records are tested through the wallet account address, after testing the owner's records, it will separate into the different pages that can reach it by clicking on a button (created by me) and creating a file in memory stored in all records, which have been confirmed its for the owner by the address that the owner created it.

The fifth shared withowner: -the fifth function is a function that fetches the records that have been shared with the owning doctor. In this function, the records are called and use a counter represents the total number of records, and another counter counts the records that have been shared with the owner doctor. In the beginning, we call a pre-established function to ensure that the doctor's address is within the list of licensed doctors to display the specified record, and then if the condition is met and the doctor's address is within the list. In this case, the record is placed within the file allocated in the memory for the files shared with the owner doctor.

3.2.1. Testing smart contract

Remix IDE is a solidity development environment used to write, compile and debug solidity code, the remix IDE was utilized for the testing of the smart contract the powerful capabilities of remix IDE make it possible for smart contracts to be tested and debugged before deployment, this ensures that the logic behavior and the smart contract state function appropriately. For purposes of testing, two different ethereum addresses were used, i.e., developer that creates the DApps use the first address to represent the owner doctor that create records 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db, the second address for doctor have permission to fetch the specific record 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2 each has 100 ether to evaluate the contract's code. A contract's state is checked before each function call is made to ensure they are executed in the correct order. Once the smart contract has been compiled and tested, the developer deploys it.

3.3. Connecting between backend and front end

In this step the connection procedure was performed, the hardhat project was created. Hardhat is a development environment designed to test, build, debug, and deploy ethereum blockchain-based decentralized applications,the idea of using a hardhat in our project is because it is considered an environment that connects the back end with the front end and tests them together, if a project develops, this setting is also very ideal for development. The site was connected to a local network for testing purposes through a setup page established for the hardhat project,the project was tested by utilizing the free hard hat accounts, in addition, a specific file for the API was developed and referenced within the hardhat configuration. A web3 library was used to link the website to the metamask wallet, and the account used depends on the network used for testing, the binance smart chain (BSC) test network was used for testing, and it is considered an environment in which DApps may be tested, it is in charge of triggering all of the BSC main net's conditions,they are used to test the project after linking it to the provider,upon its success, the project becomes ready to upload the project to a main network. Connecting the SC to the ethereum blockchain network is essential, and the ethers.js library was utilized for this purpose, all smart contracts require deployment before being utilized; ethers.js was used to enable contract calling, and the contract may be obtained through its address. To store medical records consisting of photos and pdf files in IPFS and ensure that the project has dedicated storage space, we require a provider to link the project to IPFS through the ethers.js library. The infura website was used to supply the provider by registering an account and creating a project in IPFS. After registration, it supplied us with the required information for the connection, the process of connecting and creating record is shown in Algorithm 3.

Algorithm 3. Creating record

```
Input:-[name, hash of image, hash of pdf]
Output:-create record and save in blockchain
*Initialization
*Set the name of record
name < ---- value [text]
Begin
Step 1: - upload the image and pdf.
1.1 upload the image and pdf
Begin
Disabled < ---------- loading || create record % Calling the create record task
OnChance < --------- handle input (file)
Preview Icon < ----------- values. Image file && photo Icon
Preview Icon < ----------- values.pdf file && Document Icon
Icon < --------- folder Icon
Accept < ----------- ‶image /*″
Accept < ----------- ‶.pdf*″
Step 2: - Verify that all fields are filled correctly
Step 3: - save the image and pdf on the IPFS and obtain IPFS hash URL
 hashed Image < -------   IPFS Hash Url (values. Image File)
 hashedPdf < --------- IPFS Hash Url (values. Pdf File)
Step 4: - call the contract using the address of logged –in doctor
Contract < --------- get contract (signer)
Step 6: - call the function of created record from the contract
Set created record (true)
Contract.creat record(values.name, hashed image, hashed pdf)
Step 7: - create record
Set created record(true)
END
```

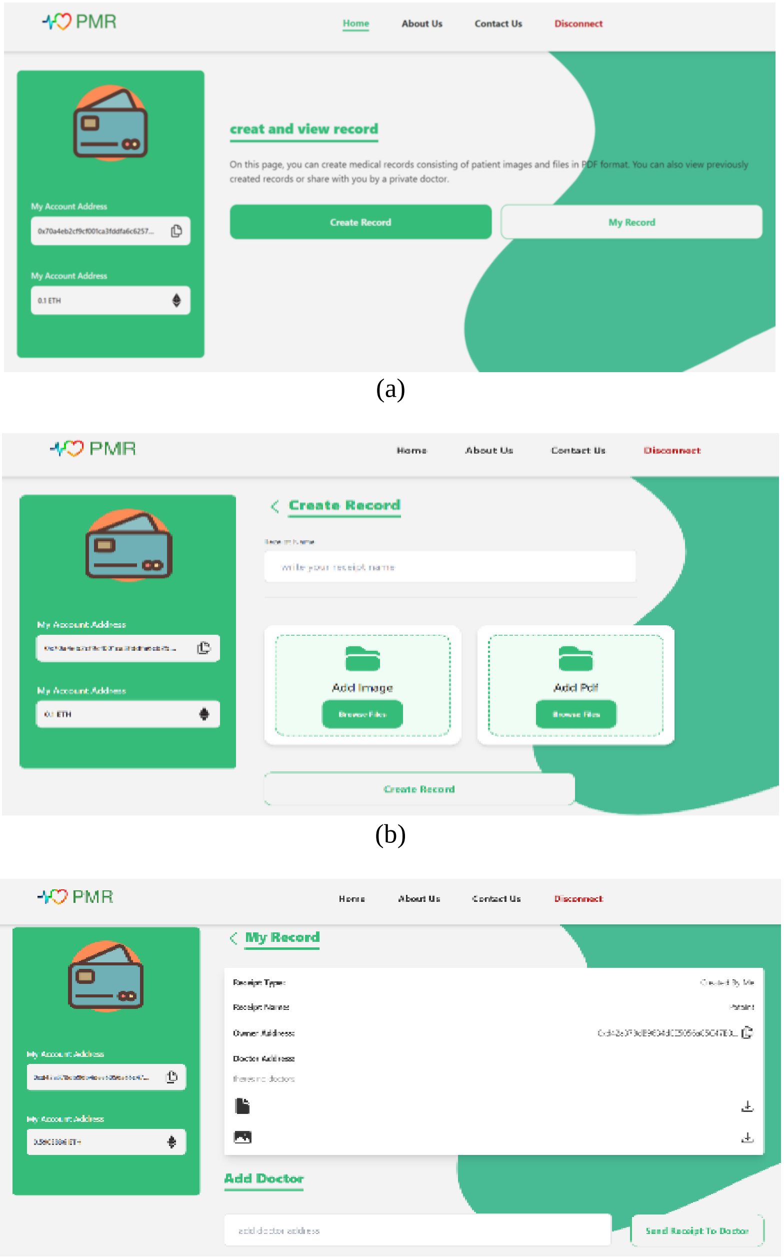
4. RESULTS AND DISCUSSION

This part aims to prove the effectiveness of the proposed system for protecting medical records, as the Figure 5 shows the he general look of the site, Figure 5(a) shows the site's appearance after logging in via the metamask. It shows the site the possibility of creating the record as in the Figure 5(b) and displaying the created and participating records. The user can also share the record he created by putting the person's address to be granted the possibility of displaying the specified record and giving him the license for that is shown in the Figure 5(c).

The proposed system stores medical records, including medical images and PDF documents, decentralized so no external party controls them and makes them globally available. IPFS provided this functionality. The records can be reached only by their owner, and the possibility of sharing these records with high security through the smart contract, as the proposed system provides security of storage, access, and sharing, in addition to reducing the cost of cloud-based storage, as seen in [21]. It relied solely on providing high security in accessing and sharing data stored in the cloud system with high privacy. The smart contract was used to share data between cloud service providers securely. Xia *et al.* [22], an information management system was proposed to address patient information by utilizing consensus mechanisms within the blockchain. This proposal aimed to mitigate energy and network congestion while prioritizing data privacy and sharing by implementing a control protocol. Jabarullah and Lee [3], the system used IPFS and smart contract technology on the blockchain platform to ensure secure storage and control of access to patient's medical images.

This approach provided enhanced security measures for storing, accessing, and sharing medical image data while reducing storage costs. The PMR system was improved by designing an integrated website that could be considered a database based on blockchain technology, which included storing images and files. Each doctor could be he has such a rule in his account in the wallet to ensure that his patients' data is permanently saved and ensure that their privacy is preserved and shared only with specialists, thus providing security of storage, access, and sharing at the lowest cost compared to current systems, the Table 1 show the comparison between PMR and related solution.

The proposed system has proven its efficiency in protecting medical records by testing it in the binance test net network. Authorized persons can only view the records; no medical record can be created except through the person who owns the site. The cost of creating the medical record is 0.0028989 BNB, and the transaction cost of granting a license to another person is 0.00071922 BNB.



On this page, you can create medical records consisting of patient images and files in PDF format. You can also view previously created records or share with you by a private doctor.

My Account Address: 0x70a4eb2cf9cf001ca3fddfa6c6257...

My Account Address: 0.1 ETH

(a)

write your receipt name

(b)

Receipt Type: Created By Me

Receipt Name: Patient

Owner Address:

Doctor Address:

there is no doctors

add doctor address

(c)

Figure 5. The general look of the site: (a) the front end of the site when log in, (b) create record, and (c) add permission

Table 1. Comparison between PMR and related solutions

Refrences	cost	Safety in sharing	Safe storage	Access to data
Xia *et al.* [22]	✕	✓	✕	✓
Fan *et al.* [23]	✓	✓	✕	✓
Shen *et al.* [24]	✕	✓	✕	✕
Jabarulla and Lee [3]	✓	✓	✓	✓
Mhamdi *et al.* [26]	✕	✕	✕	✓
(Proposed system) PMR	✓	✓	✓	✓

4.1. Performance measures

To test the efficiency of the proposed system, several measures were used, considered the most important objectives for which the system was designed, and it has been compared with previous works, analysis of the results of the proposed system is shown in Table 1, and its performance metrics are explained in subsections 4.1.1, 4.1.2, and 4.1.3.

4.1.1. Data accessibility and security

In the proposed system, the records can be reached only by their owner, this privacy was controlled through the smart contract, and the user’s address was used in the wallet to ensure it was valid for access. Many different addresses were tried in the proposed system. No one could log in and view the data. However, only the owner of the wallet and the owner of the original address is the only one who can log in and access medical records consisting of private pictures of patients and reports in PDF format about their cases and display them.

4.1.2. Safe storage of data

Decentralized storage and worldwide accessibility are key features of the proposed system for storing and sharing medical records, such as medical photographs and PDF documents. This feature was made available by IPFS. The records are confidential and can only be viewed by the owner.

4.1.3. Safety in sharing

The approach that has been proposed delivers the maximum possible security while maintaining full confidentiality of the shared data. A smart contract managed this functionality, and the address of the other doctor was used as an identifier to provide him access to the record that can only be accessed by the doctor who owns the data. Additionally, the other doctor is permitted for each record needing medical consultation regarding a special condition. In particular, the site was tested by taking a link to the record or medical pictures and documents and attempting to display the contents by addresses not authorized to display the specified record. No one could view the record, which is the most important feature that smart contracts offer their users.

4.1.4. The cost

The proposed system was based on decentralized blockchain technology, which led to cost reductions by eliminating the costs associated with maintaining and securing central storage systems. This technology enables direct peer-to-peer interactions, which enables storage without intermediaries; consequently, the costs associated with this aspect are lower than those associated with that aspect with central storage systems. The proposed system’s storage costs are acceptable.

5. CONCLUSION

Blockchain technology has become increasingly popular due to its superior security and privacy protection, this technology is regarded as a multidisciplinary approach due to its involvement in various fields such as security, internet of things (IoT), artificial intelligence (AI), and healthcare systems. This paper proposed a website to store and share medical records confidentially and securely. Blockchain technology was used to ensure decentralization and confidentiality of sharing records from one doctor to another, the ethereum blockchain and smart contract were used to give a permission only to the doctor responsible for his condition to create a record and to other doctors to view this record only to diagnose the case and these records are saved in IPFS. The proposed system has enabled the creation of a reliable medical database that offers improved efficiency and data integrity while also allowing for the sharing of medical records with security. The model for storing and sharing data is decentralized, thereby obviating the necessity of involving third-party intermediaries. The results showed by the site that records can be stored and shared easily, quickly and in complete confidentiality, and no unauthorized person can view any medical record. Blockchain technology may reduce data storage costs, but it has drawbacks. These include scalability, energy usage, and data accessibility against storage efficiency, also, there are many potential attacks against smart contracts, so it is necessary to find protection protocols to prevent intruders from accessing and manipulating these contracts. In our future research's aim is addressing these issues to make blockchain-based data storage systems more cost-effective and provide enough protection to the smart contract.

REFERENCES

[1] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, 2016, pp. 1–10.

[2] H. Tang, N. Tong, and J. Ouyang, "Medical images sharing system based on blockchain and smart contract of credit scores," in *Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking, HotICN 2018*, 2019, pp. 240–241, doi: 10.1109/HOTICN.2018.8605956.

[3] M. Y. Jabarulla and H.-N. J. A. S. Lee, "Blockchain-based distributed patient-centric image management system," *Applied Sciences*, vol. 11, no. 1, p. 196, 2020.

[4] Y. Sharma, "A survey on privacy preserving methods of electronic medical record using blockchain," *Journal of Mechanics of Continua and Mathematical Sciences*, vol. 15, no. 2, pp. 32–47, 2020, doi: 10.26782/jmcms.2020.02.00004.

[5] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021, doi: 10.1016/j.ijin.2021.09.005.

[6] G. Muradova and M. Hematyar, "Protecting and securing medical records using blockchain technology." *Informasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri*, pp. 66–69, 2019, doi: 10.25045/ncinfosec.2019.15.

[7] W. M. Lee, "Beginning ethereum smart contracts programming," *Beginning Ethereum Smart Contracts Programming*. 2019, doi: 10.1007/978-1-4842-5086-0.

[8] S. Manglekar and H. A. Dinesha, "Block chain: an innovative research area," in *Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018*, 2018, pp. 1–4, doi: 10.1109/ICCUBEA.2018.8697717.

[9] N. Khan, H. Aljoaey, M. Tabassum, A. Farzamnia, T. Sharma, and Y. H. Tung, "Proposed model for secured data storage in decentralized cloud by blockchain ethereum," *Electronics (Switzerland)*, vol. 11, no. 22, p. 3686, 2022, doi: 10.3390/electronics11223686.

[10] I. L. H. Alsammak, M. F. Alomari, I. S. Nasir, and W. H. Itwee, "A model for blockchain-based privacy-preserving for big data users on the internet of thing," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 2, pp. 974–988, 2022, doi: 10.11591/ijeecs.v26.i2.pp974-988.

[11] S. Muthurajkumar, A. Vignesh, S. Kugan, and R. Arunsha, "Decentralized web hosting service using IPFS and ethereum blockchain," in *Advances in Parallel Computing*, 2022, no. 41, pp. 58–65, doi: 10.3233/APC220008.

[12] P. Á. Costa, J. Leitão, and Y. Psaras, "Studying the Workload of a Fully Decentralized Web3 System: IPFS," In *IFIP International Conference on Distributed Applications and Interoperable Systems*, 2023, pp. 20–36, doi: 10.1007/978-3-031-35260-7_2.

[13] M. D. Praveen, S. G. Totad, M. Rashinkar, R. Ostwal, S. Patil, and P. M. Hadapad, "Scalable blockchain architecture using off-chain IPFS for marks card validation," *Procedia Computer Science*, vol. 215, pp. 370–379, 2022, doi: 10.1016/j.procs.2022.12.039.

[14] K. Salah, A. Alfalasi, and M. Alfalasi, "A blockchain-based system for online consumer reviews," in *INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019*, 2019, pp. 853–858, doi: 10.1109/INFCOMW.2019.8845186.

[15] X. Dong, "A method of image privacy protection based on blockchain technology," in *International Conference on Cloud Computing, Big Data and Blockchain, ICCBB 2018*, 2018, pp. 1–4, doi: 10.1109/ICCBB.2018.8756447.

[16] M. N. M. Bhutta *et al.*, "A survey on blockchain technology: evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[18] A. R. Poonja, S. K. Ashish, S. R. Pujar, and S. Kini, "A study on blockchain technology and its applications," *Journal of Engineering Research & Technology* 2019.

[19] S. M. Joshi and K. Rajeswari, "Efficient and accurate property title retrieval using ethereum blockchain," in *Lecture Notes on Data Engineering and Communications Technologies*, 2020, vol. 39, pp. 424–438, doi: 10.1007/978-3-030-34515-0_45.

[20] P. Karuppusamy, I. Perikos, F. Shi, and T. N. Nguyen Editors, "Sustainable communication networks and application proceedings of ICSCN 2020," in *Lecture Notes on Data Engineering and Communications Technologies*, 2021, pp. 65–72.

[21] A. S. Shibghatullah, H. K. Fatlawi, S. Kadhim, M. Falih, N. S. Ali, and A. H. Alhilali, "A comparative analysis and performance evaluation of web application protection techniques against injection attacks," *International Journal of Mobile Communications*, vol. 18, no. 1, p. 1, 2020, doi: 10.1504/ijmc.2020.10019530.

[22] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[23] 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, pp. 1–11, 2018, doi: 10.1007/s10916-018-0993-7.

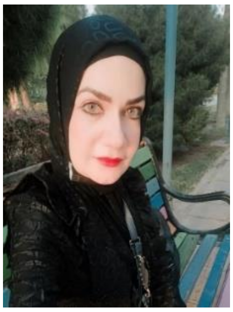
[24] B. Shen, J. Guo, and Y. Yang, "MedChain: efficient healthcare data sharing via blockchain," *Applied Sciences (Switzerland)*, vol. 9, no. 6, p. 1207, 2019, doi: 10.3390/app9061207.

[25] 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, doi: 10.1177/1460458218769699.

[26] H. Mhamdi, M. Ayadi, A. Ksibi, A. Al-Rasheed, B. O. Soufiene, and S. Hedi, "SEMRAchain: a secure electronic medical record based on blockchain technology," *Electronics (Switzerland)*, vol. 11, no. 21, p. 3617, 2022, doi: 10.3390/electronics11213617.

[27] H. M. Abdullah and A. M. Zeki, "Frontend and backend web technologies in social networking sites: Facebook as an example," in *Proceedings - 3rd International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2014*, 2014, pp. 85–89, doi: 10.1109/ACSAT.2014.22.

BIOGRAPHIES OF AUTHORS



Marwa Sami Mohammed was born in 1988 AD. She studied a bachelor's degree in computers from the University of Kufa in Iraq. She obtained a bachelor's degree in 2010 and studied a higher diploma in mathematics at the College of Computer Science and Mathematics. She works as a teaching assistant at Imam Al-Kadhim College in Iraq and is currently studying a master's degree in the department of computing in the College of Computer Science and Mathematics at the University of Kufa. Her research interests are in decentralized applications and image processing. She can be contacted at email: marwa.mawash@student.uokufa.edu.iq.

Asaad Noori Hashim is a teacher at the College of Computer Science and Mathematics at the University of Kufa. He obtained a bachelor's degree in computer science from the University of Babylon in 2001 and obtained a master's degree from the University of Babylon in 2006, and obtained a doctorate in 2015. He headed the computer department in the College of Computer Science and Mathematics for seven years. He specialized in artificial intelligence and digital image processing. Most of his research interests are in digital image processing. He can be contacted at email: asaad.alshareefi@uokufa.edu.iq.