ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 2, April 2022, pp.346-357

Securing medical records based on inter-planetary file system and blockchain

Mahmood K. Mohammed[1], Alharith A. Abdullah[2], Zaid A. Abod[1]
[1] College of Food Science, Al-Qasim Green University, Babil, Iraq
[2] Department of Information Security, University of Babylon, Babil, Iraq

ABSTRACT

In general, health records include important information like the patient's history, findings of examinations and assessments, diagnosis reports, documentation of consent, and treatment plans. Sharing this information has grown to be a challenge concerning data security, as it could result in compromising patient privacy. Therefore, the patient's information should not be misused or tampered with. In this paper, a full process of storing and retrieving medical records is proposed using a decentralized system through the integration of two emerging technologies: Blockchain and Inter-Planetary File System (IPFS). The system provides solutions for the major security concerns associated with medical files, including authentication and authorization, database breaches, data integrity of local and cloud storage, and data availability. The obtained results indicate a high level of safety by adding security layers such as confidentiality, authentication, authorization and access control, based on different factors. All these aspects contribute to reaching the aim of the proposed system, which is storing and retrieving medical records in a decentralized and safe manner.

Keywords: Blockchain, IPFS, Medical records, Smart contract, Decentralized application

Corresponding Author:

Mahmood K. Mohammed
College of Food Science
Al-Qasim Green University
Babil, Iraq
E-mail: mahmood@uoqasim.edu.iq

1. Introduction

Nowadays, the Internet has become almost the most important part of daily life. It is used to communicate with friends and colleagues, to learn online, to run a business and much more. The current web stores data and information in a centralized approach. In this approach, data is stored in big farms of servers, which are usually owned and controlled by one company or organization. The centralization brings several problems and issues, including availability and censorship. To address these problems and issues, the way of accessing information should be changed. This requires a file-sharing protocol that allows users to get a copy of the file even if the server is down. Instead of informing the computer where to find the information or resources, the computer can state what the information is. This method is known as Content-Based Addressing and is called IPFS. Another technique handling the problems of centralization is blockchain, which is a decentralized storage system providing multiple features such as privacy, immutability, integrity, and consistency. These are significant criteria for any system.

Thus, the use of these techniques in many fields has become a major research concern. One of these areas is the health sector, where a large amount of medical data is generated that must be archived, disseminated and consulted on a daily basis. At the same time, this information has to be kept confidential. Besides, it must not change. The criteria for transparency in archiving medical records requires a structure that provides easy maintenance and access to data.

Presently, many researchers used the IPFS and blockchain in multiple domains based on the features in both technologies. In [1] the authors used the IPFS for storing digital content like multi-media files in a distributed way, providing public and global access to everyone. The IPFS hash is deployed in Ethereum blockchain smart contracts for ensuring that the process is integral original, and authentic. Blockchain and IFS are used in decentralized publishing systems of open science. This system provides a distributed system for reviews, in addition to Open Access by-design infrastructures and a governing process of high transparency [2]. The researchers in [3] deal with medical images where they introduce a framework for eliminating third-party intermediaries to share records and store them on the networks securely. An open asymmetric encryption technique is used for hashing and protecting the content of images. A combination of a voting-based consensus algorithm and decentralized file sharing system is used. The proposal in [4] depends on using Ethereum smart contracts for governing and regulating the document versions of control functions between the document's creators, developers, and validators. It aims towards facilitating multi-user collaborations and tracking changes in a centralized way with trust and security, with no need for third parties to be involved. The research in [5] related to developments in exchanging personal health data systems in a secure way by using smart contract authorized security on the basis of the blockchain and the IPFS to help build efficient healthcare systems. The authors in [6] created an attribute-based encryption system for securely storing and efficiently sharing electronic medical records in IPFS. The proposal is determined by the cypher-text policy attribute encryption, for the effective control of access to electronic medical data with no effect on retrieval efficiency. At the same time, the encrypted electronic medical data is stored in the decentralized InterPlanetary File System (IPFS), thereby solving the issue of single-point failures. The researchers in [7] presented a system including an Ethereum blockchain and IPFS-based decentralized framework to store and share access to medical images. The suggested system provides facilitation to patients to access a medical database of immutability, with more data provenance and efficient audits, in a highly efficient way, in addition to shared access to medical images. The researchers here also used Blockchain-based smart contracts and IPFS for enabling patients to control their medical data immutably, transparently, traceably, and securely, in a decentralized way [8]. A group of researchers stored medical data in a distributed, off-chain manner by means of IPFS and blockchain. The suggested framework preserves patient privacy while facilitating access to medical data by authorized entities like health providers [9]. There are a number of problems and challenges related to the Electronic Medical Record (EMR) systems, in terms of securing, accessing and managing data. These aspects are addressed through the suggested combination of blockchain and IPFS System solution framework for EMR in the health industry [10]. In [11], the system of the blockchain and IPFS is proposed in an IoT environment, whereby the blockchain is used for storing the evidence of services, whereas IPFS is utilized for storing and sharing data in a secured way.

This work makes use of blockchain technology, which represents a modern research trend showing prospective results for securing the data when shared. Given the fact that blockchain provides anonymity, immutability and decentralization of data, the deployment of smart contracts and access controlling programs are useful for monitoring data activity within blockchain networks. The IPFS is used, which is an emerging technology represented by a decentralized peer-to-peer storage system. It is applied for storing digital content of medical records integrally so as to be accessed globally. The outline of the paper can be sketched in the following way: Sections 2 and 3 explain the concepts of blockchain and IPFS respectively. Section 4 presents the proposed scheme. As for Section 5, the experiment results and evaluation are provided. Section 6 compares the proposed scheme. The concluding remarks are stated in Section 7.

2. Blockchain

Blockchain technology is getting significant attention in industrial and academic fields. Important aspects to be described are what blockchain is, how it works, what issues it solves, and the manner in which it could be applied in other fields. In order to understand this technology, the aforementioned aspects are to be discussed.

This technology was firstly described in 1991 by a research team, with an initial intention of timestamping digital documents so that it is not backdated or tampered with [12]. Then in 2009, it was used to create the digital cryptocurrency Bitcoin [13]. As its name indicates, it is a chain of information blocks and a distributed ledger that is utterly open to anyone with a significant property, which is data immutability.

All blocks contain the following elements: data, current block hash, and the hash of the previous block. The type of data stored within the blocks is determined by the blockchain type. To exemplify, the Bitcoin blockchain stores the transaction details like the senders, receivers, and amount of coins. The hash represents a unique digital fingerprint of the block which defines the block and its contents. After creating the block, any changes to its contents will cause the hash to be changed. The third component of all blocks is the hash of the previous block which produces the chain of the blocks in an efficient way. This technique is the reason behind the blockchain's security.

Therefore, a blockchain is a distributed database that could be used to create a permanent and unchangeable record of transactions. It eliminates the single points of failure as it stores data in a decentralized approach [14]. It is not just for cryptocurrencies anymore, since there are several types of blockchain depending on the way it is built [15]. It can be used in many other industries and applications to solve problems that are found in the current world [16]. It uses a decentralized system of data storage [17], [18].This means it has no central server and no central administrator to manage its data. Instead, it relies on peer-to-peer networks to share information across the internet [19]. This means that blockchain is not only difficult for individuals or entities to tamper with, but it also makes sure that no single points of failure occur in the system [20], [21].

Blockchain is a decentralized platform for data storage. This means that it is possible to store any type of data on the blockchain. The most important property of blockchain that makes it an appealing option for data storage is its decentralization [22]. The system does not have a single point of failure, so if one node goes offline, the network can still continue to grow and store information. It can also store medical data in an unchangeable manner. This will allow doctors to access this information without any risk of corruption or hacking. However, the blockchain approach has its own limitations, such as it is inefficient to store files of large sizes. Another issue is that the process of storing and retrieving data on the blockchain using smart contacts is quite expensive in terms of money and power [23].

3. Inter-planetary file system

Interplanetary File System is a peer-to-peer file system whose aim is to make the web faster and more stable while also making it easier for people to share files without having to worry about hosting or bandwidth [23], [24]. It is designed for storing files in a versioned and decentralized manner. IPFS can be used as a distributed web protocol with a fast and secure distributed database for applications like websites, web stores, and payment systems [25]. This section explains how IPFS deals with files and explains the benefits of using IPFS and its immutability.

A file is broken into smaller pieces whenever it is uploaded to IPFS. A unique identifier called Content Identifier (CID) is generated using a cryptographic hash function [26]. IPFS relies on DHT (Distributed Hash Table) which is a distributed system that maps CID to peer addresses that have the content (key-value mapping, CID to IP address/port) [27]. For instance, “ipfs://x” is a request to access a file with CID “x” which query the DHTs to retrieve all peers that have that particular CID. DHT is stored on all connected nodes and is updated whenever any changes occur. Whenever a node seeks out a file, it enquires about its other peer nodes in the network that store the content of the file’s CID. For example, in figure (1) there are three nodes present in the network storing distributed DHT, and three different files. However, not every node has a copy of all files. If Node A wants to get a copy of the file CID3, the DHT points to node C since it is the only one that has this file. After node A gets the file with CID3 and caches it, then the DHT will be updated consequently and it will become a provider of the file number 3 until its cache is cleared [28] as figure (2) Illustrates.

Every node in IPFS has a unique identifier represented by the hash of its public key. It can pin content with the purpose of storing and seeding it permanently. Unpinned content will be removed when it has not been used for a given period of time, with the purpose of saving storage space. Therefore, every node controls the contents that it stores and seeds.

IPFS has many features and attributes, a few of which are stated below:

- Resistant to tampering: Once the data is added to the IPFS, it is immutable to changes since any update on the file will result in an utterly different CID.
- Censorship: Data is stored in a distributed manner and there is no one party that has full control over a certain file.
- Offline use: Visiting or viewing the data is enough to catch the data within the IPFS network, and there is no need to get it every time from its initializer.
- Bandwidth efficiency: Feature number 3 will save plenty of bandwidth, as other nodes will get data from the nearest node that has cached the data.
- IPNS: As stated above, IPFS utilizes content-based instead of location-based addressing. It relies on CID to identify the content which is a long string. This string is changed every time a new version of the file is added. Hence, the IPFS provides a decentralized name system called InterPlanetary Name System. IPNS solves this problem by creating an updateable address.

Hospitals must have a precise full history of the patient records. One of the most important features of the IPFS protocol is immutability. Once the data is stored on IPFS nodes, there is no way to take it down or change it unless all nodes stop hosting it, which is difficult to achieve. In order to update the hosted data on IPFS, it is necessary to make new versions of it without deleting it. Such features bring plenty of advantages to be utilized for storing medical records as data will be permanent on the web and unchangeable.

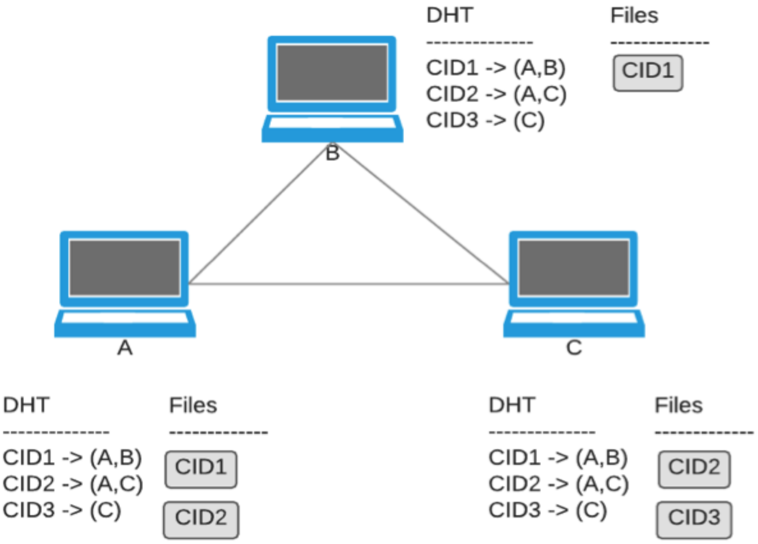


Figure 1. The distributed hash table in IPFS network

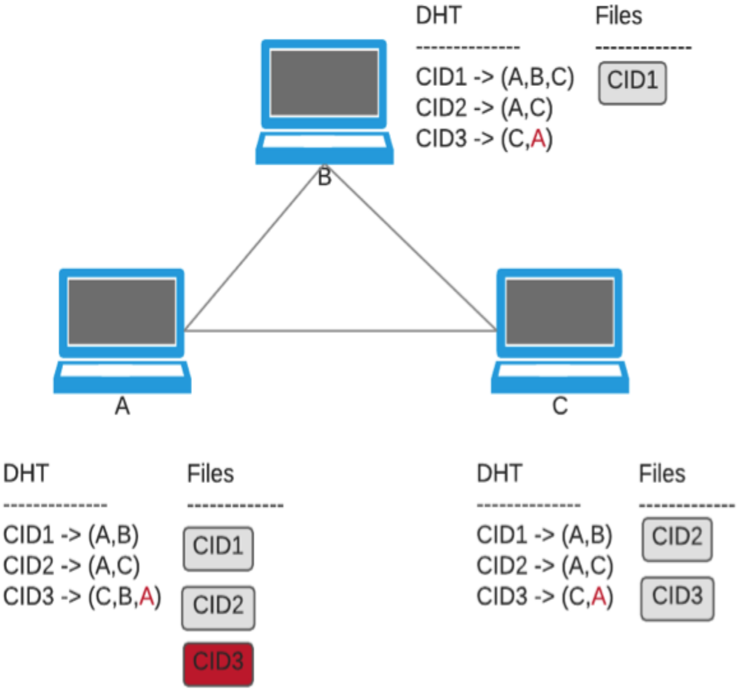


Figure 2. Updates on DHT after node A requested and acquired a

copy of the file with CID 3

4. Proposed system architecture

The proposed system consists of two phases, including the full process of storing and retrieving files or media using the proposed decentralized system. The system provides solutions for the major security concerns associated with medical files, including authentication and authorization, database breaches, data integrity of local and cloud storage, and data availability.

First phase: In order to add a new file to the system, the user (hospital, patient or IoMT) must have a blockchain wallet address to be verified as a valid user. The first step is encrypting the file to ensure data confidentiality. The system uses asymmetric or public-key cryptography. The process of encryption is done as follows:

- Generating new pares of private and public keys.
- Using the public key to encrypt the file.
- Encrypting the generated private key through the patient's public key.
- Rerunning the last step using the hospital public key.

The aim of encrypting the generated private key is to give authorization to the right parties that can decrypt and open the file after extracting the generated private key using their own private key. The latter is associated with their blockchain wallet account.

In the second step, and after the encryption process is finished, the file will be uploaded to a remote or local IPFS node. IPFS, in turn, will hash the file using one of the hashing algorithms such as SHA-256, and then returns the hash as CID (content identifier). In this stage, the system guarantees data integrity since the CID works as a unique identifier and any data editing or manipulation will cause to generate a completely different CID. Furthermore, the system fulfils the demand of ensuring data availability, as the file will be immutable on IPFS.

In the third step, the system uses Ethereum smart contract to store the following information to Blockchain after using the user blockchain wallet account to sign the transaction:

- CID
- File name or description.
- Patient blockchain wallet address.
- The generated private key is encrypted with the patient public key.
- The generated private key is encrypted with the hospital public key.

In this phase, the aim of the system is to store a few pieces of information on the blockchain for reducing the cost and time compared to the cost and time required for storing the actual files on the blockchain, as shown in figure (3).

In the second phase, the process of retrieving a file is divided into three main steps. Firstly, the user requests a file or full list of the patient's transactions (transactions that contain the patient's blockchain wallet address) using an Ethereum smart contract. The returned information from blockchain is a specific transaction or a list of transactions in which each transaction consists of a set of information, as illustrated in figure (4).

In the second step, the user will use the CID (a hash of the required file) to request the file from any IPFS node that has the requested CID in its DTH. Then, the IPFS node will reply with an encrypted copy of the required file. By performing the two aforementioned steps, the required file will be on the user's device.

However, in the third step, the user must decrypt the file in order to see its contents, as the file was encrypted when it was uploaded to the IPFS using one-time-use pair of public-private keys. Consequently, and firstly, depending on who the user is (whether a patient or a hospital), the associated private key of the user is to be utilized to decrypt the generated private key. Then, the generated private key will be used to decrypt the requested file, as shown in figure (5).

The algorithms of storing process and retrieving process are shown in figures (3 and 5) and summarized in the following algorithms:

```
Algorithm 1: Storing a file on IPFS node
Input: File, patient public key, hospital public key
Output: File hash (CID), decryption keys, file name.
Begin:
```

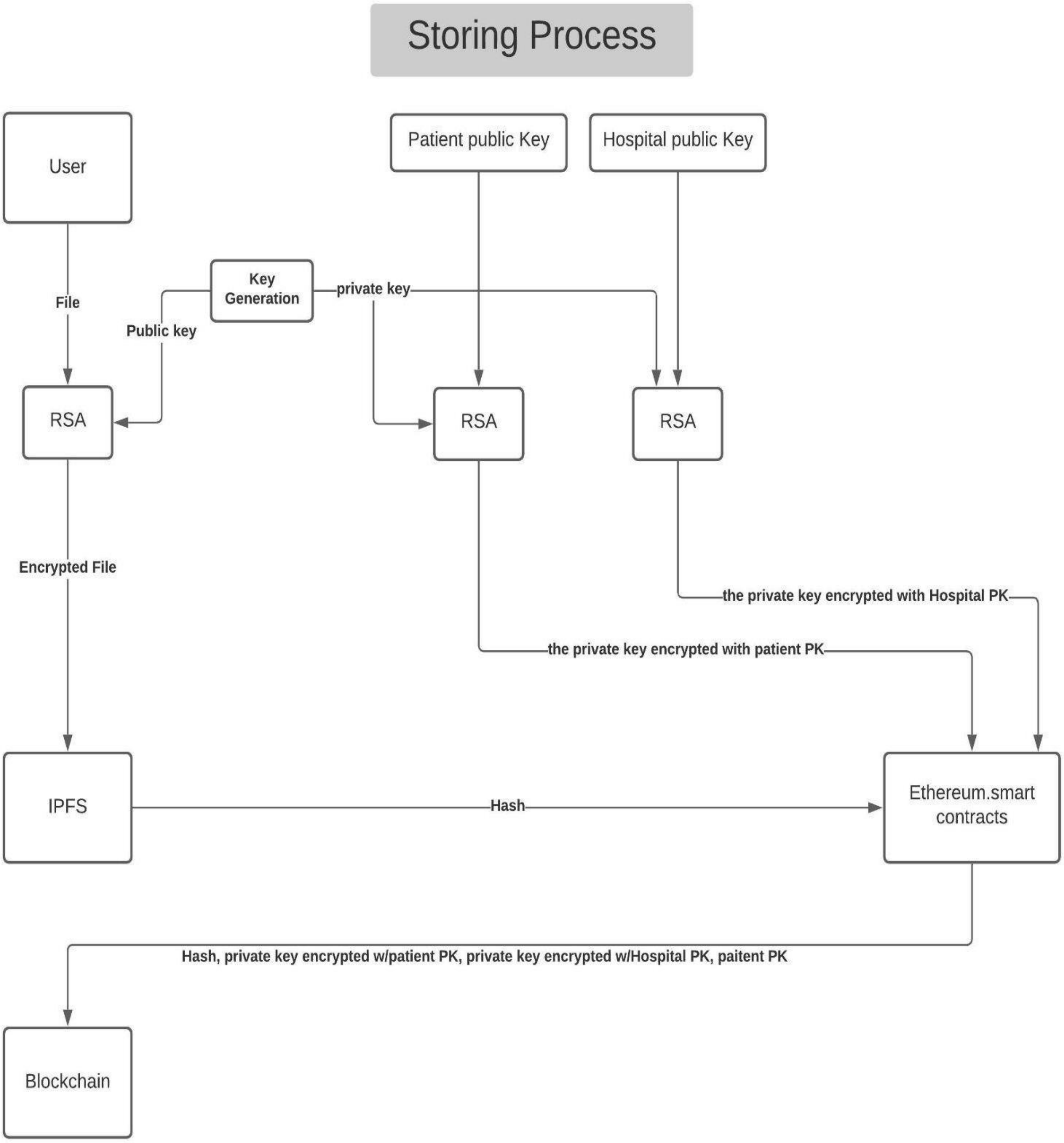

Storing Process
User
Patient public Key
Hospital public Key
File
Key Generation
private key
Public key
RSA
RSA
RSA
Encrypted File
the private key encrypted with Hospital PK
the private key encrypted with patient PK
IPFS
Hash
Ethereum.smart contracts
Hash, private key encrypted w/patient PK, private key encrypted w/Hospital PK, paitent PK
Blockchain

Figure 3. Flow diagram of storing medical records in the proposed solution

Step 1: Capture the file.
Step 2: Encrypting the file as follows:

1. Generate new pair of one-time-use pair of public-private keys.
2. Encrypted the file using the public key of the generated pair.
3. Encrypt the private key of the generated pair using the patient’s public key
4. Encrypt the private key of the generated pair using Hospital’s public key

Step 3: Upload encrypted file to IPFS node.
Step 4: Get the CID back from the IPFS node.
Step 5: Store CID, PDK, HDK, patient wallet address and file name to the personal Blockchain.
End

Algorithm 2: Retrieving a file from the IPFS node
Input: The patient wallet address, filename (optional), the hospital or patient public key.
Output: File.
Begin:
Step 1: Get CID from the blockchain using the patient wallet address.
Step 2: Get the encrypted file from the IPFS node using CID.
Step 3: Decrypt the private key using either patient or hospital private key.
Step 4: Decrypt the file using the private key.
End

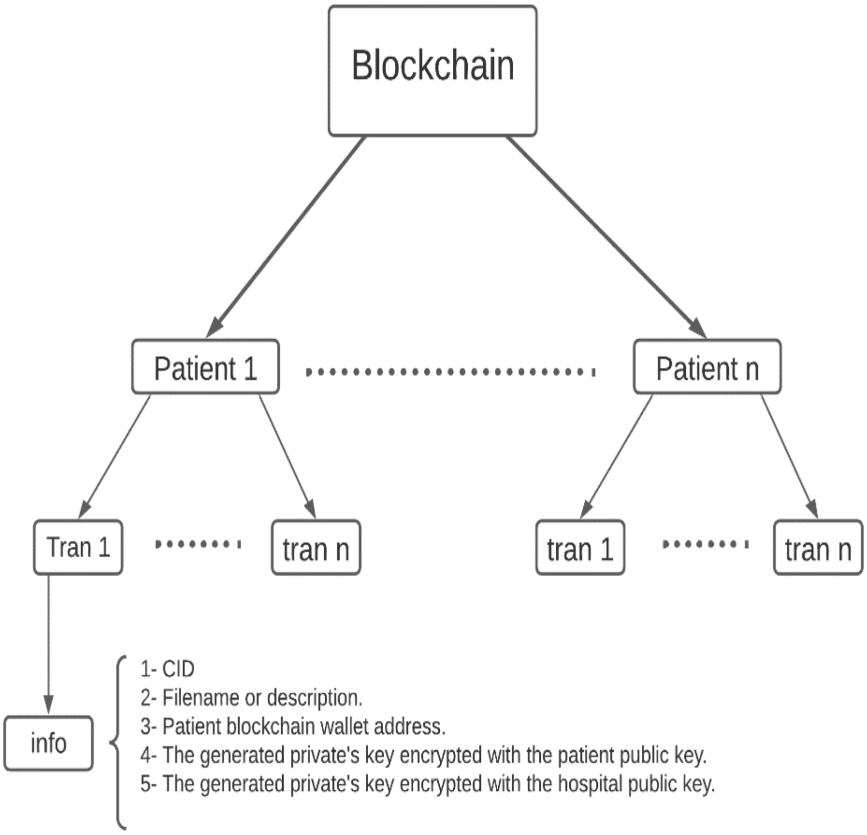

Blockchain
Patient 1
Patient n
Tran 1
tran n
tran 1
tran n
info
1- CID
2- Filename or description.
3- Patient blockchain wallet address.
4- The generated private's key encrypted with the patient public key.
5- The generated private's key encrypted with the hospital public key.

Figure 4. Overview of the structure of the stored on-chain data

5. Experimental results and evaluation

As aforementioned, the proposed system is a decentralized application (DApp) storing and retrieving data in a decentralized manner. Hence, to achieve the goal of the system, a set of tools and programming languages are utilized, including Node.js, React, Truffle suite, Ganache, Solidity, MetaMask, IPFS-HTTP-client, HTML and Bootstrap.

Truffle allows the utilization of packages that are capable of testing, compiling and deploying smart contracts straightforwardly on blockchain networks. These features make Truffle one of the best platforms that suit the need of this work. The React box from Truffle is used, which contains all the necessaries that are required to run smart contracts from React application. In addition, Ganache is used as a personal Ethereum blockchain. Then, the Web3.js and MetaMask extension on Chrome are utilized to establish the connection between the DApp and the Ethereum node (in this case, Ganache).

After building the smart contract using solidity, it was compiled and deployed to Ganache using Truffle. Then, the IPFS-HTTP-Client library is employed to establish the connection between the DApp and a local or a public IPFS node.

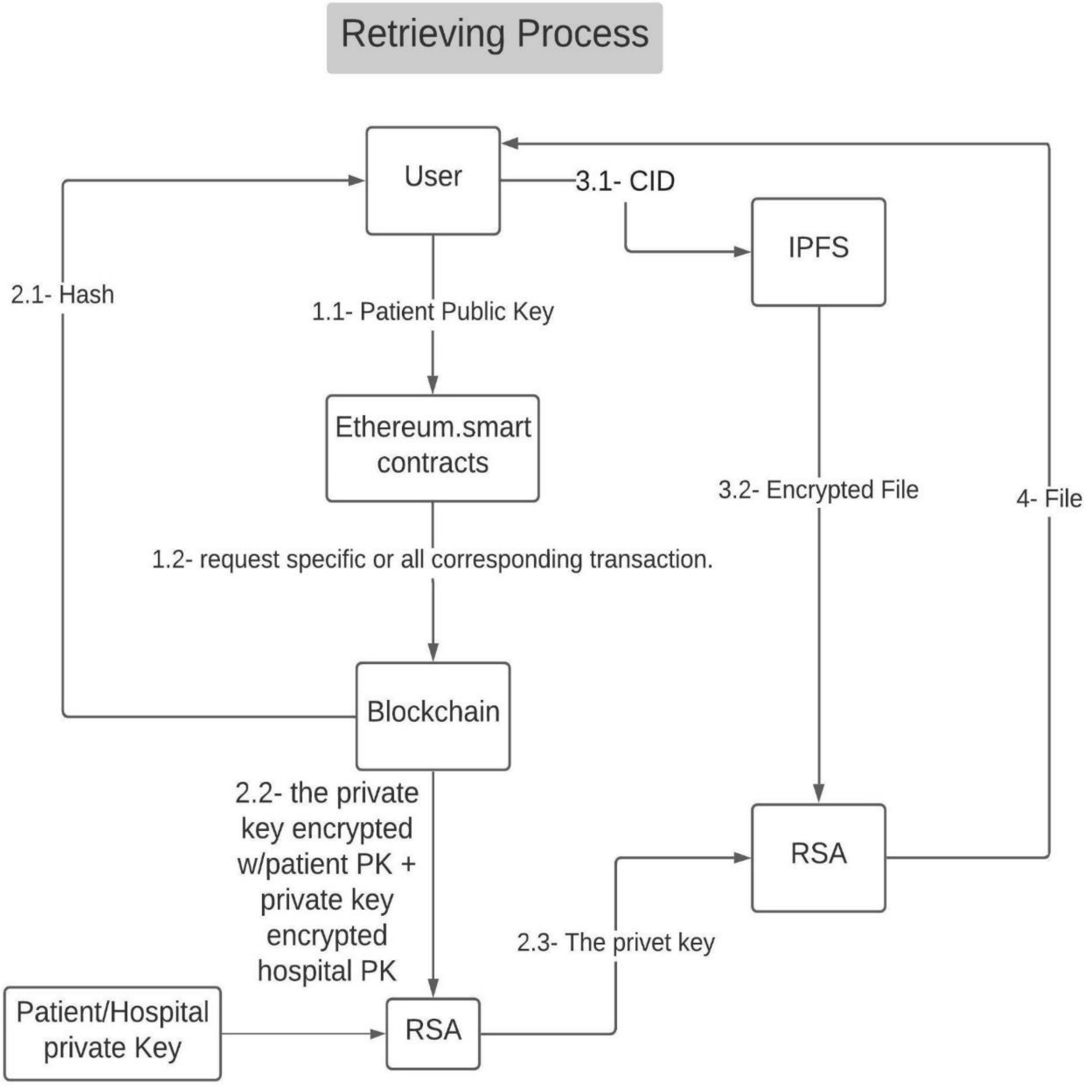

Retrieving Process
User
3.1- CID
IPFS
2.1- Hash
1.1- Patient Public Key
Ethereum.smart contracts
3.2- Encrypted File
4- File
1.2- request specific or all corresponding transaction.
Blockchain
2.2- the private key encrypted w/patient PK + private key encrypted hospital PK
RSA
2.3- The privet key
Patient/Hospital private Key
RSA

Figure 5. Flow diagram of retrieving medical records in the

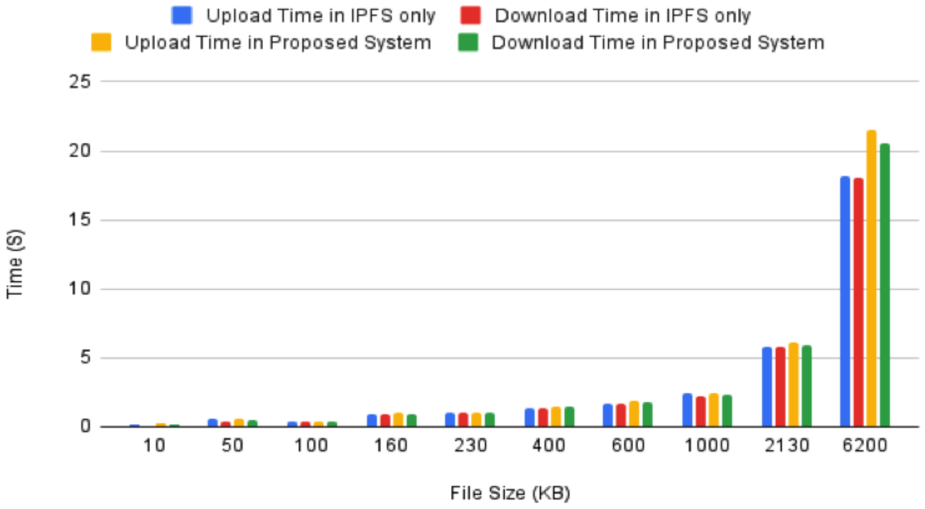
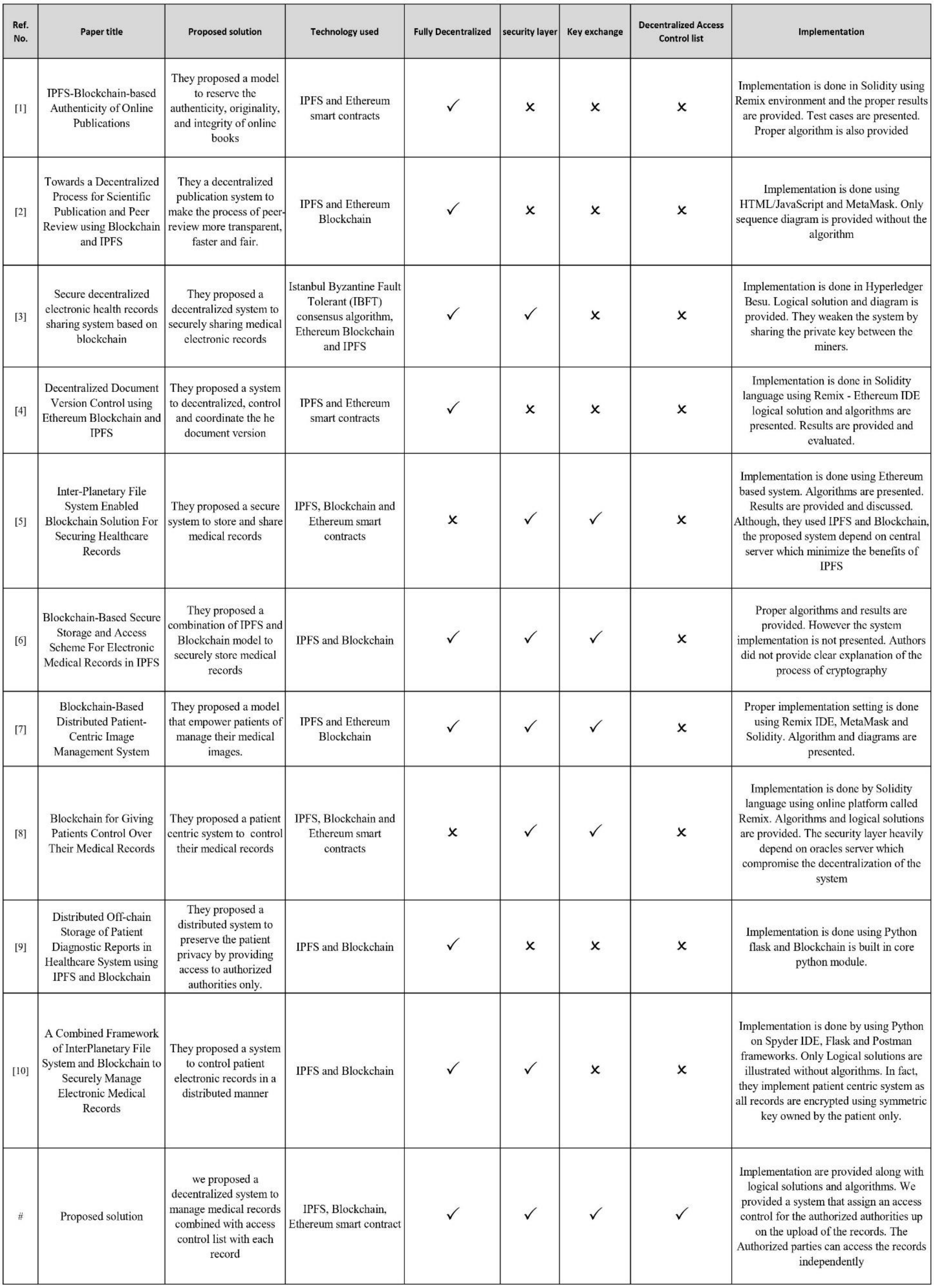


Figure 6. Column chart for comparing adding files of different sizes to IPFS and proposed system

Table 1. Comparison with other schemes



Ref. No.	Paper title	Proposed solution	Technology used	Fully Decentralized	security layer	Key exchange	Decentralized Access Control list	Implementation
[1]	IPFS-Blockchain-based Authenticity of Online Publications	They proposed a model to reserve the authenticity, originality, and integrity of online books	IPFS and Ethereum smart contracts	✓	✗	✗	✗	Implementation is done in Solidity using Remix environment and the proper results are provided. Test cases are presented. Proper algorithm is also provided
[2]	Towards a Decentralized Process for Scientific Publication and Peer Review using Blockchain and IPFS	They a decentralized publication system to make the process of peer-review more transparent, faster and fair.	IPFS and Ethereum Blockchain	✓	✗	✗	✗	Implementation is done using HTML/JavaScript and MetaMask. Only sequence diagram is provided without the algorithm
[3]	Secure decentralized electronic health records sharing system based on blockchain	They proposed a decentralized system to securely sharing medical electronic records	Istanbul Byzantine Fault Tolerant (IBFT) consensus algorithm, Ethereum Blockchain and IPFS	✓	✓	✗	✗	Implementation is done in Hyperledger Besu. Logical solution and diagram is provided. They weaken the system by sharing the private key between the miners.
[4]	Decentralized Document Version Control using Ethereum Blockchain and IPFS	They proposed a system to decentralized, control and coordinate the he document version	IPFS and Ethereum smart contracts	✓	✗	✗	✗	Implementation is done in Solidity language using Remix - Ethereum IDE logical solution and algorithms are presented. Results are provided and evaluated.
[5]	Inter-Planetary File System Enabled Blockchain Solution For Securing Healthcare Records	They proposed a secure system to store and share medical records	IPFS, Blockchain and Ethereum smart contracts	✗	✓	✓	✗	Implementation is done using Ethereum based system. Algorithms are presented. Results are provided and discussed. Although, they used IPFS and Blockchain, the proposed system depend on central server which minimize the benefits of IPFS
[6]	Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS	They proposed a combination of IPFS and Blockchain model to securely store medical records	IPFS and Blockchain	✓	✓	✓	✗	Proper algorithms and results are provided. However the system implementation is not presented. Authors did not provide clear explanation of the process of cryptography
[7]	Blockchain-Based Distributed Patient-Centric Image Management System	They proposed a model that empower patients of manage their medical images.	IPFS and Ethereum Blockchain	✓	✓	✓	✗	Proper implementation setting is done using Remix IDE, MetaMask and Solidity. Algorithm and diagrams are presented.
[8]	Blockchain for Giving Patients Control Over Their Medical Records	They proposed a patient centric system to control their medical records	IPFS, Blockchain and Ethereum smart contracts	✗	✓	✓	✗	Implementation is done by Solidity language using online platform called Remix. Algorithms and logical solutions are provided. The security layer heavily depend on oracles server which compromise the decentralization of the system
[9]	Distributed Off-chain Storage of Patient Diagnostic Reports in Healthcare System using IPFS and Blockchain	They proposed a distributed system to preserve the patient privacy by providing access to authorized authorities only.	IPFS and Blockchain	✓	✗	✗	✗	Implementation is done using Python flask and Blockchain is built in core python module.
[10]	A Combined Framework of InterPlanetary File System and Blockchain to Securely Manage Electronic Medical Records	They proposed a system to control patient electronic records in a distributed manner	IPFS and Blockchain	✓	✓	✗	✗	Implementation is done by using Python on Spyder IDE, Flask and Postman frameworks. Only Logical solutions are illustrated without algorithms. In fact, they implement patient centric system as all records are encrypted using symmetric key owned by the patient only.
#	Proposed solution	we proposed a decentralized system to manage medical records combined with access control list with each record	IPFS, Blockchain, Ethereum smart contract	✓	✓	✓	✓	Implementation are provided along with logical solutions and algorithms. We provided a system that assign an access control for the authorized authorities up on the upload of the records. The Authorized parties can access the records independently

The proposed system will be evaluated in terms of the time required to store and retrieve data. All experiments are performed by deploying the smart contract on a local Ethereum blockchain network, followed by uploading files to a public IPFS node.

The experiment set is CPU Intel Core i5-3230M, 6G DDR3 Memory with a network connection of the following properties: upload/download speed 2.25Mbps and latency 101ms.

Several files of different sizes were used to test the latency in the upload/download process to IPFS, with and without the process of encryption/decryption and storing/retrieving CID to/from the blockchain. A range of 50-6200 KB is uploaded several times throughout the proposed solution with the purpose of measuring the required time to encrypt, upload files to the IPFS node and store transactions on the local blockchain. Then, several files were downloaded using CID from the blockchain and decrypted using the private key of the user.

Figure (6) illustrates the variations of the required times to upload/download files to IPFS, both with and without using the proposed solution. As the file size is increased, the uploading/downloading time is consequential increasing and vice versa. In the process of using pure IPFS, the time differential between the two tasks is insignificant. On the other hand, when using the proposed system, there is a slight time increase in the task of uploading files. The cause of this increment is due to the process of granting access permissions to the potential users.

It is unfair to compare the proposed solution results to the relative works, as it is difficult to meet the experiment's environment settings. Logically, there will not be a live session between the hospital and the patient since the purpose of storing medical records is to be utilized later either by the hospital or the patient. Consequently, the use of pure public key cryptography to secure the files access is not enough. Therefore, in this work, a simplified access control layer is added. In Table 1 summarizes an evaluative comparison that will be drawn between the capability of the proposed scheme and alternative ones.

6. Conclusion

Blockchain and IPFS are relatively recent developments that promise prospective results in various applications and fields. This paper presents a system that proposes the implementation of the decentralized application (DApp) for storing and retrieving medical records based on blockchain and the advancement of IPFS technology. The proposed system is an explanation for using smart contracts and access control mechanisms for the effective security of medical records stored on IPFS nodes and retrieved from IPFS nodes, based on an asymmetric encryption system (represented by the RSA algorithm). The system provides multiple security objectives, such as authentication, authorization, integrity and availability although the latency is slightly increased, hence a secure healthcare environment.

Funding information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

References

[1] N. Nizamuddin, H. R. Hasan, and K. Salah, “IPFS-blockchain-based authenticity of online publications,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10974 LNCS, pp. 199–212. doi: 10.1007/978-3-319-94478-4_14.

[2] A. Tenorio-Fornés, V. Jacynycz, D. Llop, A. A. Sánchez-Ruiz, and S. Hassan, “Towards a decentralized process for scientific publication and peer review using blockchain and IPFS,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2019, vol. 2019-January, pp. 4635–4644. doi: 10.24251/hicss.2019.560.

[3] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, “Secure decentralized electronic health records sharing system based on blockchains,” *Journal of King Saud University - Computer and Information Sciences*, vol. In Press, pp. 1–14, May 2021, doi: 10.1016/J.JKSUCI.2021.05.002.

[4] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, “Decentralized document version control using ethereum blockchain and IPFS,” *Computers and Electrical Engineering*, vol. 76, pp. 183–197, 2019, doi: 10.1016/j.compeleceng.2019.03.014.

[5] R. K. Marangappanavar and K. Kiran, “Inter-Planetary File System Enabled Blockchain Solution for Securing Healthcare Records,” in *ISEA-ISAP 2020 - Proceedings of the 3rd ISEA International Conference on Security and Privacy 2020*, 2020, pp. 171–178. doi: 10.1109/ISEA-ISAP49340.2020.235016.

[6] J. Sun, X. Yao, S. Wang, and Y. Wu, “Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS,” *IEEE Access*, vol. 8, pp. 59389–59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[7] M. Y. Jabarulla and H. N. Lee, “Blockchain-based distributed patient-centric image management system,” *Applied Sciences (Switzerland)*, vol. 11, no. 1, pp. 196–216, 2021, doi: 10.3390/app11010196.

[8] M. M. Madine *et al.*, “Blockchain for Giving Patients Control over Their Medical Records,” *IEEE Access*, vol. 8, pp. 193102–193115, 2020, doi: 10.1109/ACCESS.2020.3032553.

[9] R. Kumar, N. Marchang, and R. Tripathi, “Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain,” in *2020 International Conference on COMmunication Systems and NETworkS, COMSNETS 2020*, 2020, pp. 1–5. doi: 10.1109/COMSNETS48256.2020.9027313.

[10] A. al Mamun, M. U. Faruk Jahangir, S. Azam, M. S. Kaiser, and A. Karim, “A combined framework of interplanetary file system and blockchain to securely manage electronic medical records,” in *Advances in Intelligent Systems and Computing*, 2021, vol. 1309, pp. 501–511. doi: 10.1007/978-981-33-4673-4_40.

[11] H. Zareen, S. Awan, M. B. E Sajid, S. M. Baig, M. Faisal, and N. Javaid, “Blockchain and IPFS Based Service Model for the Internet of Things,” in *Lecture Notes in Networks and Systems*, 2021, vol. 278, pp. 259–270. doi: 10.1007/978-3-030-79725-6_25.

[12] A. Whitaker, “Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts,” *Artivate: A Journal of Enterprise in the Arts*, vol. 8, no. 2, pp. 21–46, 2019, doi: 10.34053/artivate.8.2.2.

[13] S. Singh and N. Singh, “Blockchain: Future of financial and cyber security,” in *Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016*, 2016, pp. 463–467. doi: 10.1109/IC3I.2016.7918009.

[14] S. Kumar, A. K. Bharti, and R. Amin, “Decentralized secure storage of medical records using Blockchain and IPFS : A comparative analysis with future directions,” *Security and Privacy*, vol. 4, no. 5, pp. 162–178, 2021, doi: 10.1002/spy2.162.

[15] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, “Blockchain technology in healthcare: A comprehensive review and directions for future research,” *Applied Sciences (Switzerland)*, vol. 9, no. 9, pp. 1736–1764, 2019, doi: 10.3390/app9091736.

[16] A. A. Abdullah and W. K. Oleiwi, “A SURVEY OF THE BLOCKCHAIN CONCEPT AND MITIGATION CHALLENGES IN DIFFERENT NETWORKS,” *Journal of Hunan University（Natural Sciences）*, vol. 48, no. 10, pp. 890–905, 2021, [Online]. Available: https://www.researchgate.net/publication/355351692

[17] Z. Zheng *et al.*, “An overview on smart contracts: Challenges, advances and platforms,” *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020, doi: 10.1016/j.future.2019.12.019.

[18] H. A. Jawdhari and A. A. Abdullah, “The Application of Network Functions Virtualization on Different Networks, and its New Applications in Blockchain: A Survey,” *Webology*, vol. 18, no. Special Issue 04, pp. 1007–1044, Sep. 2021, doi: 10.14704/WEB/V18SI04/WEB18179.

[19] H. A. Jawdhari and A. A. Abdullah, “A novel blockchain architecture based on network functions virtualization (NFV) with auto smart contracts,” *Original Research*, vol. 9, no. 4, pp. 834–844, 2021.

[20] R. Kumar and R. Tripathi, “Blockchain-Based Framework for Data Storage in Peer-to-Peer Scheme Using Interplanetary File System,” in *Handbook of Research on Blockchain Technology*, 2020, pp. 35–59. doi: 10.1016/b978-0-12-819816-2.00002-2.

[21] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, “A secured distributed detection system based on IPFS and blockchain for industrial image and video data security,” *Journal of Parallel and Distributed Computing*, vol. 152, pp. 128-143., 2021, doi: 10.1016/j.jpdc.2021.02.022.

[22] N. Nizamuddin and A. Abugabah, “Blockchain for automotive: An insight towards the IPFS blockchain-based auto insurance sector,” *International Journal of Electrical and Computer Engineering*, vol. 11, no. 3, pp. 2088–8708, 2021, doi: 10.11591/ijece.v11i3.pp2443-2456.

[23] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, “Blockchain-Based, Decentralized Access Control for IPFS,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1499–1506. doi: 10.1109/Cybermatics_2018.2018.00253.

[24] N. Fotiou, V. A. Siris, and G. C. Polyzos, “Enabling self-verifiable mutable content items in IPFS using Decentralized Identifiers,” in *2021 IFIP Networking Conference, IFIP Networking 2021*, 2021, pp. 1–6. doi: 10.23919/IFIPNetworking52078.2021.9472820.

[25] S. Khatal, J. Rane, D. Patel, P. Patel, and Y. Busnel, “FileShare: A Blockchain and IPFS Framework for Secure File Sharing and Data Provenance,” in *Algorithms for Intelligent Systems* , 2021, pp. 825–833. doi: 10.1007/978-981-15-5243-4_79.

[26] H. Mukne, P. Pai, S. Raut, and D. Ambawade, “Land Record Management using Hyperledger Fabric and IPFS,” in *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, 2019, pp. 1–8. doi: 10.1109/ICCCNT45670.2019.8944471.

[27] H. M. Hussien, S. M. Yasin, N. I. Udzir, and M. I. H. Ninggal, “Blockchain-based access control scheme for secure shared personal health records over decentralised storage,” *Sensors*, vol. 21, no. 7, pp. 2462–2498, 2021, doi: 10.3390/s21072462.

[28] H. Ye and S. Park, “Reliable vehicle data storage using blockchain and ipfs,” *Electronics (Switzerland)*, vol. 10, no. 10, pp. 1130–1145, 2021, doi: 10.3390/electronics10101130.