

A survey: medical health record data security based on interplanetary file system and blockchain technologies

Rana Abbas Al-Kaabi^{1,2}, Alharith A. Abdullah¹

¹College of Information Technology, University of Babylon, Babil, Iraq

²Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq

Article Info

Article history:

Received Sep 13, 2022

Revised Dec 16, 2022

Accepted Dec 20, 2022

Keywords:

Availability

Blockchain

Confidentiality

Integrity

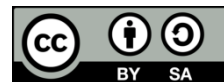
Interplanetary file system

Medical health record

ABSTRACT

The adoption of modern health records is growing more mature, yet security issues always accompany it. Interplanetary file system (IPFS) and blockchain are developing technologies with decentralization, distributed fault tolerance, and trustworthiness. Using IPFS and blockchain technology to tackle medical health record data security issues is a very promising trend, and it is presently being utilized to secure medical health record data security. This article first explains the idea of IPFS and highlights the classification of existing IPFS and blockchain techniques before briefly discussing distributed ledger to tackle the existing medical health record data security challenges and faults. Finally, to preserve medical health records, a new medical health record storage architectural model based on IPFS and blockchain technologies is presented.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Alharith A. Abdullah

College of Information Technology, University of Babylon

Babil, Iraq

Email: alharith@uobabylon.edu.iq

1. INTRODUCTION

Patient medical records have progressed from paper to electronic data integrity, allowing them to be kept safe, accessed, and legally authorized by only valid medical centers [1]. The amount of available health care data is rapidly increasing as medical information technology advances, this can aid individuals in disease prevention, increase the likelihood that they will be cured, give guidelines for hospitals and pharmaceutical businesses, and serve as proof in situations involving medical-legal culpability and medical conflicts. Health information sharing and use have greatly aided in the allocation of healthcare resources, clinical decision-making, medical quality monitoring, precision medicine, and disease risk assessment and prediction [2].

Transparency in archiving medical records requires a system that allows for easy data maintenance and access. This demands the use of a file-sharing protocol that allows users to retrieve a copy of the file even if the server is unavailable. The method is called IPFS and is known as content-based addressing [3].

On the blockchain, the procedure of storing and searching for medical data is documented, allowing for the tracking of both the data's original source and its retrieval [4]. Data security has become a challenge when it comes to sharing health-related data, which could put patients' privacy at risk. In most cases, once the health provider's report is complete, it is uploaded to the hospital's central system.

Many participants (all known components of any healthcare system) in the hospital as an organization require patient medical reports for various reasons. It's a difficult and challenging problem to provide a single platform where all participants can securely share confidential data. Patients' personal data should not be misused or tampered with [5]. They employ a storage technology called the interplanetary file system (IPFS) to address this issue. In order to reduce unnecessary file redundancy, the decentralized storage protocol IPFS

adds a unique hash to every file that is recorded. According to the hash address, the user can locate the corresponding file. IPFS has no single point of failure since it is decentralized. Prior to storage, they encrypt medical data various attributes, and prior to storage, we identify user attributes (as well as those of physicians, nurses, patients, and researchers) [6].

The user's private key is linked to their attributes, whereas the ciphertext is linked to the policy. The decrypting the ciphertext only if and when their private key fits the access policy within. The storage and retrieval of medical data are tracked using the blockchain, which may record both the origin of the data and the retrieval procedure. Additionally, they can keep the hash value of medical data in the blockchain, which offers solid proof that the client has confirmed the data's originality [7].

There are several reviews on the blockchain, and IPFS in medical systems have been summarized. Bigini *et al.* [8] aims to provide an overview of the current state-of-the-art blockchain-based systems for the internet of medical things (IoMT), with a focus on the problems of achieving user-centricity for these combined systems, as well as potential future directions for full data ownership by users. They looked at the contributions of blockchain to IoMT applications in their study, concentrating on the existing issues and future vision. Distributed ledger technology (DLTs) have the potential to revolutionize the way we handle privacy and security in healthcare, as well as make information sharing between institutions more efficient. Blockchain can be the driving technology for developing long-term and independent data-sharing platforms by achieving certain goals such as user-centricity, security, scalability, and interoperability. Kumar *et al.* [9] improved the storage of medical records by working on IPFS and blockchain systems, loss of data or distortion is a serious danger even though most hospitals keep patient records locally, and many don't even have backup storage. A thorough analysis of current solutions and their framework is demonstrated in this paper that will make it easier to conduct ongoing research and development on these systems. Given the recent widespread ransomware attacks on hospitals around the world, several academics are employing various strategies to address the critical problem of data security in hospitals. Researchers have developed numerous models, applications, and algorithms that handle a wide range of problems; however, the models even have serious downsides that will need to be resolved. Finding a reliable solution is necessary for expenditure, flexibility, energy conservation, strategic planning, and data access throughout emergencies. We must deal with various cyberattacks, including insider assaults and others.

The major contributions of the paper to the research field are listed below.

- We presented an efficient and safe blockchain-based approach to MHR management (i.e., transferring and storage).
- Blockchain technology has the potential to enhance existing MHR systems. Integrating blockchain with IPFS can enable existing blockchains in systems with multiple storage issues.
- Examine how the suggested model satisfies the requirements of the nodes involved (i.e., health care providers, patients, and third parties).
- To obtain a better knowledge of the system's privacy and security measures.
- To protect the confidentiality of patient reports. The re-encryption scheme helps to keep medical records private and ensures that they can only be shared with authorized doctors.

The organization of the paper can be sketched in the following way: Sections 2 and 3 explain the concepts of IPFS and blockchain respectively. In section 4 we review the main objective of security which are confidentiality, integrity, and availability (CIA). In section 5 we present our classification for the articles that use the concept of IPFS and blockchain in the medical system to deal with security objectives. Section 6 new medical health record architecture model based on blockchain and IPFS technologies the last section 7 conclusion.

2. INTER-PLANETARY FILE SYSTEM (IPFS)

Prabha *et al.* [10] The interplanetary file system (IPFS) is a hypermedia distributed storage and transport protocol that is content-addressable, versioned, and peer-to-peer. Fast download rates, worldwide storage, security, and data preservation are just a few of the benefits of IPFS. The features are as follows: IPFS simply considers the content of the file, creating a unique hash mark from it that can be accessed by the mark's uniqueness and checked beforehand to see whether it has already been stored [11]. It is obviously read from several other nodes if it was already stored, conserving space in the process. Slicing huge files: IPFS nodes are unconcerned about the storage path or name of the data they store [12]. When using IPFS to slice and dice big files, many slices can be downloaded in parallel [13]. Via storing massive-size data hypermedia on IPFS, a decentralized, distributed network topology can alleviate bottlenecks in the blockchain's storage capacity. IPFS adds a cryptographic hash to encrypted data that is unique to digital content, and the recorded file's associated hash cannot be changed [14]. The hash is a one-to-one match with the file. The location of the server, as well as the file's name and path, are irrelevant in an IPFS network. Whenever the file is put into an IPFS node, it

receives a distinct hash value based on its metadata. When a user requests access to a file, IPFS uses the hash table to locate the file's location and retrieve it. The blockchain storage issue might be resolved by utilizing IPFS in conjunction with blockchain [15]. IPFS structure is shown in Figure 1.

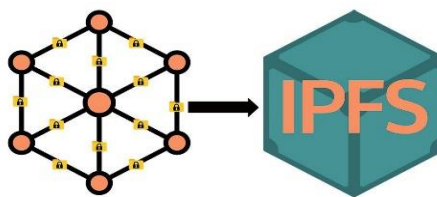


Figure 1. Inter-planetary file system (IPFS) P2P structure

3. IMMUTABLE LEDGER (BLOCKCHAIN)

A network of interconnected blocks that serves, as a distributed ledger is known as a blockchain. Each block contains an arranged series of transactions [16]. Because it works primarily through decentralization, this technology provides a new model for securely storing data [17]. A blockchain is made up of blocks of transaction information that are structured and kept in chronological order. Because all blockchain servers have a copy of the information, it is difficult to conduct malicious action against it [18]. A unique cryptography hash binds the new block to the preceding blocks. If the content of a block is changed, the previous block will still include the hash of the next block. To hide the modification on one block, the hacker needs to change all subsequent blocks for a significant number of machines that have a copy of the blockchain [19]. As a result, the information on the blockchain is safe and unalterable. Blockchain technology has proven to be a reliable and secure method of storing transactions [20]. The blockchain was first used for the digital currency Bitcoin. Decentralized applications (DApps) were created to take advantage of this database for data storage and retrieval. These applications rely on decentralized databases based on the blockchain rather than a central database. As a result, there is no single point of failure (NSOF) [21].

The following are the essential elements of blockchain: transaction: In blockchain, a transaction represents the operation that the user performed on the network [22]. It's crucial to figure out what data should go on-chain and what should stay off-chain [23]. A block is a grouping of valid transactions and their related data. It's important to note that each blockchain has its own set of block fields; however, many blockchains include the following: (This is the block's header; this is the block's data.) The block is then transmitted to all network peers after it has been validated [24]. In any blockchain, a genesis block is the first block. Mining refers to the process of adding a new block (transaction) to the blockchain. Miners (individual network nodes) create blocks with authorized transactions and add them to the blockchain [25].

The consensus algorithm: Consensus algorithms allow distributed systems to communicate safely. Various consensus techniques are used by different blockchain networks. Proof-of-work (PoW), which is used in Bitcoin, and proof-of-stake (PoS), which is used in Ethereum, are the most well-known. The main advantage of PoS vs PoW is that it uses significantly less power and hence is more cost-effective. Autonomy, trust, and disintermediation are the three key advantages of Building decentralized data-sharing and deployment capabilities with distributed ledger technology [26].

The multiple main fundamental procedures of insertion, elimination, update, and inquiry make up the entirety of the management of medical archive information. Intelligent contracts have the power to alter users' behavior and encourage constructive participation in the exchange of medical information [27]. This integration of adaptive contract and block link technologies can increase the mechanization of historical knowledge transfer via various forms of blockchain [28].

There are standard types of immutable ledger which are:

- Public blockchain (permissionless); This upholds the idea that data is accessible to all in the world. A consensus procedure is necessary to post or block evidence to the press blockchain [29].
- Consortium blockchain(hybrid); This is a private party. Rather than being managed by a single entity, something is managed by a group. The ability to read blockchain data is either open or constrained to a few select individuals [30].
- Private blockchain: That just a select group of participants is permitted to add data to the public ledger. The data is accessible to both the public at large and a limited number of customers [31]. Blockchain types as shown in Figure 2.

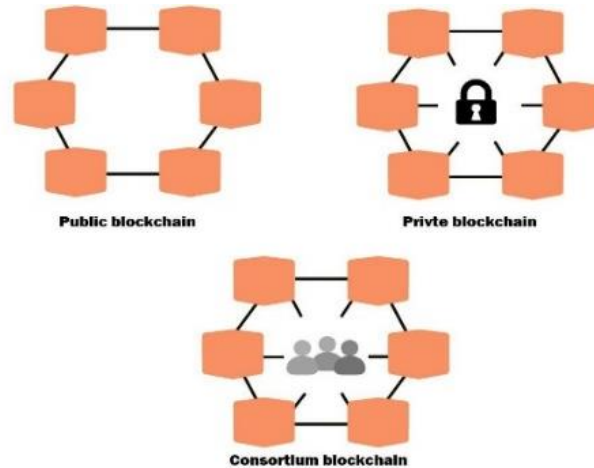


Figure 2. The structure of blockchain technology types

4. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)

The CIA model outlines the three primary goals of cybersecurity. The letter C stands for confidentiality. Data and information privacy is essential for cybersecurity. Usernames, password combinations, medical histories, and other data, files, and staff must be permitted or confined to specific people, equipment, or procedures. Though many issues might arise if the wrong people get access to information and data users really aren't supposed to have seen, confidentiality is focused on the accessing of data and information. In the CIA paradigm, the letter I stands for integrity. Users ought to be ensured that the information that is transferred analyzed and stored has still not been altered, either unintentionally or forcibly. For example, whenever a message is modified in one place, it can modify everywhere [32]. The overall transmission could even be twisted or unintelligible. It means that the final letter of the alphabet is available. Availability guarantees that users who are permitted to perform their work can do so even with all of the cybersecurity precautions in place for working with equipment, software, individuals, procedures, and therefore more. Legitimate people should have immediate access to the tools they should be doing their work, and in the event of a cybersecurity incident or catastrophe, the system should be completely resilient and load-balanced [33]. CIA security is shown in Figure 3.



Figure 3. The main objectives of security (security triangle: confidentiality, integrity, and availability)

5. EXAMPLES OF MODERN MHR DATA SECURITY SOLUTIONS USING IPFS AND BLOCKCHAIN TECHNOLOGY

In order to preserve patients' security, it is of utmost importance to understand how patients' data are stored, shared, used, and managed by using IPFS and distributed ledger technology which is blockchain technology in the healthcare industry. In the following subsections, we divided down into specific categories including confidentiality of MHR data, Integrity of MHR data, and authentication of MHR data respectively, in each subsection we listed numerous pieces of research that proposed multiple ideas on how to use IPFS and blockchain technology in the healthcare system.

5.1. Maintain the confidentiality of MHR data

Battah *et al.* [34] proposed a system consisting of entities that communicate with the smart contracts to govern the access control of the encrypted data stored on the IPFS. By securing the information with a cryptographic algorithm and delivering it to the P2P decentralized repository in with another key encrypted by the public key of a shared wallet among authorized users and the proprietor of the data utilizing multi-signature, the suggested scheme maintains confidentiality. In addition, the creator of the data generates a smart contract that includes the hash of the aforementioned parts, which serves as the data's address. The owner of the data then generates a re-encryption key using its private key and the public key of the requestor to submit to the proxy servers. The data is downloaded by the client application from the proxies. It then goes on to decrypt both the data and the symmetric key has used its private key before decrypting the data once and using more than the symmetric key.

Sun *et al.* [35] constructed a technique for attribute-based encryption. Their technique, which effectively restricts access to electronic medical records while maintaining retrieval effectiveness, is based on ciphertext policy attribute encryption. In the interim, they keep confidential electronic medical records in the distributed interplanetary file system (IPFS). They used a range of operations, such as encryption, indexing, storage, and retrieval, to represent the full system.

Madine *et al.* [36] hypothesized that decentralized, immutable, transparent, traceable, and secure smart contracts built on the blockchain offer patients ownership over their medical data. The majority of existing personal health records (PHR) management strategies and systems are centralized. They not just to make it extremely difficult to share medical data, but they also run the risk of creating a single point of failure. The suggested system makes utilization of reputation-based re-encryption oracles and interplanetary file systems (IPFS). Due to the anonymity all individuals and the encryption of all medical record data, the privacy of all parties, including patients, is ensured. Just one patient and their selected doctors could connect the medical records thanks to the suggested solution's stringent re-encryption mechanism, which also guarantees confidentiality.

Kumar *et al.* [37] IPFS was already proposed as a blockchain-based distributed off-chain storing system for patient diagnostic reports. The problem of protecting user privacy is the underlying storage mechanism, which is immutable and content-addressable, which is a problem with the centralized model. Unauthorized access to crucial information such as identity details and diseases from which a patient is suffering, as well as misuse of patients' data and medical reports, are all threats to user (patient) privacy. Using interplanetary file system (IPFS) and blockchain technology, the proposed system allows authorized entities, such as healthcare providers, easy access to medical data. The healthcare provider, mining process, on-chain storage, and off-chain storage are the four elements that make up the implementation. All of these modules are self-contained.

Subramanian and Thampy [38] proposed a system to solve the issue of storing diabetic patients' medical records. To maintain track of medical records, the blockchain consortium was formed. Diabetes patients' medical records are secured using the Ethereum sandbox simulation concept. To preserve the privacy of personal healthcare information, the interplanetary file system (IPFS) encrypts health data and delivers it to the blockchain. This consortium is being developed as a proof-of-concept (PoC) model using the new economy movement (NEM) symbol blockchain. As a distributed ledger acetone-butanol-ethanol (ABE) method is employed to keep medical records confidential, and each stakeholder in a consortium is assigned a NEM-produced QR code to monitor records. The aims of the project are to design a framework for secure handling of diabetes patients' health data and prioritize needs during a pandemic and apply the zero-knowledge proof algorithm to validate the transaction between stakeholders such as hospitals, vaccination centers, pharmacies, government agencies, insurance companies, and other stakeholders.

Barati *et al.* [39] designed a platform for the creation of online vaccine certificates using IPFS is proposed. Only non-sensitive data is stored within the blockchain for auditing purposes. Digital vaccine passports are one of the most important solutions for resuming travel in the post-COVID-19 world. Key challenges such as trust, scalability, and security must be overcome to implement a vaccine passport. Their proposed platform supports general data protection regulation support (GDPR) by implementing smart contracts. by IPFS. The distributed hash table (DHT) algorithm was implemented.

Raut and Shah [40] proposed that data tampering is one of the most serious problems in current technology. Although it may be possible to detect and forecast patients' states using data analytics within a single entity, handling and correlating patients' related data across various organizations is difficult. The issue isn't a lack of resources; rather, it's a lack of resource management. As if to find a solution to this problem, blockchain technology is rapidly gaining attention for the security of confidential data. The main concern with this proposed methodology is protecting patients' data effectively. For this purpose, interplanetary file system (IPFS) is used in conjunction with the Ethereum blockchain. The proposed system was developed with the help of the Ethereum blockchain, which stores patient-related data on IPFS. Now, the privacy of patients' data is

increasing. The whole control is in the patient's hand. The model is patient-centric. The patient can approve or disapprove of the doctor, as well as allow him/her to see previous histories and add new records. The use of IPFS increases its capability to store large amounts of data. In the future, the system will also arrange appointments, bookings, payments, and insurance. System integration is done using the Ethereum blockchain.

Mani *et al.* [41] offered an inventive approach that consists of off-chain solutions that securely store actual health data over the interplanetary file system while encrypting it in an on-chain health record database (IPFS). Due to privacy, confidentiality, and security concerns, the development of blockchain-based electronic health systems is constrained. They do this by describing PCHDM, an end-to-end secure health record chain network architecture, and its design, implementation, and evaluation. To guarantee the security of health records amongst stakeholders, the architecture combines networks, IPFS, and smart contracts. The system that has been put into place seems effective and meets several security standards. It is possible to achieve a high level of confidentiality, transparency, and reliability.

Majdoubi *et al.* [42] Per the researcher, the internet of things (IoT) is changing the healthcare industry through accelerating sharing, including the use of client records and incorporating service users. Though they can access and exchange their private health data from anywhere, patients are now more satisfied and motivated with IoT-enabled devices. That new approach makes medical care provision increasingly feasible by enabling machine-to-machine connectivity, interoperability, data mobility, and medical interchange. To preserve privacy in data sharing in an s-healthcare system, they created and deployed smart med chain, an end-to-end blockchain-based architecture. Patients' medical IoT data will be transmitted and monitored, and clinicians can access it with their permission. To guarantee scalability, we only retain the hash of health records on the blockchain; the actual data is saved after encryption in the distributed storage system IPFS. The analysis' conclusions show that the suggested solution is workable and satisfies many regulatory standards. The likelihood that it will maintain health data security, transparency, confidentiality, consistency, and flexibility is the highest

Sheeraz *et al.* [43] presented a blockchain-based architecture for gathering healthcare data. In the first phase, the participants for data collection will be registered on the blockchain. In the second phase, they will be collected using a software application. Then the data will be encrypted and stored on IPFS after the identity verification of the data sender. After successful storage of data, the data index of IPFS will be stored on the blockchain network. In this way, only authorized participants can participate in data collection, and accurate data will be collected. The data stored on IPFS is secured and can only be identified by the indexes that are stored on the blockchain. Since healthcare data is sensitive, they used encryption techniques to encrypt the data. Every user in the system has to register on the network, and a private and public key pair will be issued to the users. These key pairs will be used as credentials to interact with the system. They have used the dApp concept to make data consistent and structured.

Azbeq *et al.* [44] presented a chronic disease management system based on IoT, blockchain, and IPFS technologies. This method has a number of advantages in terms of remote patient monitoring. It collects, shares, and protects data on a daily basis. There are three pieces to the system. The first side is in charge of data gathering. To ensure collection, this side is utilizing IoT healthcare gadgets. The second side is in charge of safely sharing data. Blockchain is the technology that makes this possible. The final side is for data storage, and it employs IPFS. Any healthcare system can benefit from our system. However, in our situation, they chose to employ it, particularly in the treatment of chronic disease systems, because this type of condition requires daily follow-up and regular check-ups. The suggested system is completely decentralized, and it provides a high level of security by utilizing blockchain, smart contracts, proxy re-encryption, and IPFS to regulate access to patient data, preserve privacy, and assure data integrity (Clique proof of authority (PoA) algorithms, PoW algorithm). The whole paper summarizes in Table 1.

5.2. Verify MHR data integrity

Jabarulla and Lee [45] in the field of health care, medical images are stored and exchanged. Current procedures rely on cloud-based centralized space and cause privacy problems when sharing data over a network. The researchers presented a proof-of-concept architecture for the proposed patient-centric image management (PCIM) system, which is a decentralized framework based on the Ethereum blockchain and IPFS for storing and distributing medical pictures. It was designed for a distributed PCIM system that aims to keep data safe and control it without relying on a central system. Use the PCAC-SC management system, which allows authorized entities to access blockchain data. They encrypt the sensitive medical images before uploading them to the global IPFS network. This ensures data originality, ensures data security, and prevents data from being leaked to irrelevant users. A pair of asymmetric keys, a public and a private one, is generated. The paper summarizes in Table 2.

Table 1. Blockchain and IPFS-Based MHR data confidentiality method

Papers	Techniques used	Advantages	Disadvantages	Implementations
[34]	Ethereum blockchain, IPFS	<ul style="list-style-type: none"> ○ MHR data retain a reliable, safe, and unchangeable audit trail that anybody can check. ○ Fully decentralized. 	<ul style="list-style-type: none"> - The audit trail of MHR data is reliable, unchangeable, and secure so that anyone may check it, are really difficult. - There is no key exchange mechanism. 	Remix solidity IDE
[35]	Blockchain IPFS	<ul style="list-style-type: none"> - Secure content storage - Verifiable keyword Search access control 	<ul style="list-style-type: none"> - Access privileges and the timeliness of expired users - Functional problems with blockchain data. 	Theoretical research
[36]	Ethereum blockchain, IPFS	<ul style="list-style-type: none"> - Give patients control over their medical records in a decentralized, traceable, reliable, trustful, and secure manner. 	<ul style="list-style-type: none"> - Patients do not have full control over their data because it is stored in hospitals. - Interoperability - Key management - GDPR - Smart contracts upgradability 	Remix solidity IDE
[37]	Consortium blockchain and IPFS based off-chain storage model	<ul style="list-style-type: none"> - Provide privacy of the patient reports 	<ul style="list-style-type: none"> - Transaction upload is more computation-intensive than transaction download for all report sizes. 	Python
[38]	The NEM symbols Blockchain, IPFS	<ul style="list-style-type: none"> - Secure handling of diabetes patients' health data - Keep medical records confidential 	<ul style="list-style-type: none"> - Costly drugs - Knowledge of diabetes disease covid_19 and diabetes. - Existing healthcare system for diabetes patients during covid_19 	Theoretical research
[39]	Blockchain, IPFS	<ul style="list-style-type: none"> - Keeping and verifying patient data 	<ul style="list-style-type: none"> - Sharing vaccine passport data between different organizations, regions, and countries 	Solidity language.
[40]	Blockchain, IPFS	<ul style="list-style-type: none"> - Protecting personal data and enabling citizens to control creating, storing, and verifying digital vaccines certification 	<ul style="list-style-type: none"> - Implementation of both access control and encryption management layers of the designed architecture. - Development of the proposed platform in the cloud environment and the management of CIDs 	Solidity language. Ganache is a local test network
[41]	Web3.js, Ethereum blockchain, IPFS	<ul style="list-style-type: none"> - Protect patient's data from different illegal access - Patients have confidentiality towards their record 	<ul style="list-style-type: none"> - Data tampering - Correlating patient-related data due there is lack of resource management 	Ethereum blockchain (Ganache), solidity
[42]	Hyperledger Fabric Blockchain, IPFS	<ul style="list-style-type: none"> - Privacy, security, integrity, interoperability, and scalability are issues with patient-centric distributed architecture when storing patient-centric data. - They have developed a revolutionary algorithm for utilising blockchains to securely store and access records. - To ensure scalability and effectiveness, the initial massive amounts of data are maintained off-chain in IPFS. 	<ul style="list-style-type: none"> - The implementation of multi-blockchain systems calls for an enormous number of resources. - The system included Non-Fungible Tokens (NFT) so that stakeholders could access audio and video as NFT data. 	Node.js, Java, access control languages
[43]	SmartMedChain, blockchain, IPFS	<ul style="list-style-type: none"> - Has the capability to assure security, privacy, confidentiality, integrity, and scalability of the health data and is effective in practice while meeting various security standards. 	<ul style="list-style-type: none"> - In a broad smart healthcare ecosystem, using many Blockchains may need a lot of resources. 	Node.js web service API
[44]	Blockchain dApp, IPFS	<ul style="list-style-type: none"> - Keep data accurate, consistent, reliable, and easily accessible to the researchers - Ensure authorized access to the data. - IPFS provides secure sharing and easier accessibility of data. 	<ul style="list-style-type: none"> - The process of collecting data for research is always a difficult and time taking process. - The data is distributed, unstructured, inconsistent, and complex 	Theoretical research

Table 2. Blockchain and IPFS-Based MHR data integrity method

Papers	Techniques used	Advantages	Disadvantages	Implementations
[45]	Novel proof-of-concept design with blockchain and IPFS	<ul style="list-style-type: none"> - Allows users to have full control of their medical images by ensuring guaranteed security, transparency, and data integrity - The use of IPFS in medical image migration time and retrieval time is faster 	<ul style="list-style-type: none"> - Due to the decentralized nature of their systems, such as losing private keys. 	Solidity is a programming language that was integrated into the Remix IDE.

5.3. Perform MHR data authentication

Jabarulla *et al.* [46] proposed a decentralized solution for storing and sharing medical photos based on blockchain and IPFS. Before being posted to IPFS, the image files are encrypted using steganography and asymmetric encryption. An open asymmetric encryption approach hashes and protects the image content. In addition, we encode the patient's description on medical photographs using steganography technology.

Marangappanavar *et al.* [47] data security issues have made it difficult to share health information, which could jeopardize patient privacy. Health record management and security techniques now in use have been shown to be insufficient. They proposed an architecture for a decentralized blockchain-based PHR sharing mechanism that ensures anonymity, taking advantage of emerging technologies like IPFS. The idea shows how to use a smart contract and an access control system to adequately preserve data that may be shared with patient authorization. The system effectively functions as a multiple-access system because healthcare providers have had their own records. The system protects data and information for data protection and adherence to fundamental health sector requirements. To deploy smart contracts, a truffle suite is utilized, which provides contract addresses for contract calls. Depending on the type of request, the data owner assigns a process for translation. A transaction is created and authorized using just a private key.

Kumar and Tripathi [48] To address concerns with the the privacy risk of COVID-19 patients' information, including unauthorized access to sensitive patient data like specific results and clinical records, they proposed a distributed on-chain and off-chain storage model based on consortium blockchain and interplanetary file systems (IPFS). Large amounts of COVID-19 patient records can be potentially saved because of peer-to-peer file storage models made possible by the interplanetary file systems (IPFS). The underlying storage mechanism retains a content-addressed hash of the files and uses distributed hash table (DHT) and version-control methods to get rid of duplicate files.

Al Mamun *et al.* [49] suggested a framework for EMR in the healthcare sector that combines a blockchain and the interplanetary file system. Electronic medical record (EMR) systems confront significant concerns with data management, security, and accessibility. Unauthorized access to medical records and improper use of patient disease reports are among the many security dangers to patient privacy. Prior to submitting files to the blockchain network, the suggested solution additionally intends to minimize record volumes. Additionally, a distinctive IPFS hash and patient control over the EMR provide data immutability. The client must obtain the private key from the data owner in order to view the patient's medical records. The AES-256 method is used to encrypt the EMR. Additionally, it offers total control over the data.

Kumar and Tripathi [50] proposed that the internet of medical things (IoMT) is the next frontier in the digital revolution, and it leverages IoT in the healthcare domain. However, according to cloud-based storage, IoMT poses a significant issue for data storage management, reliability, and transparency. They suggest a consortium blockchain network with smart contract support to solve these problems. On order to initially implement smart contracts for patient and medical device authentication in the same cluster layer, they integrate interplanetary file systems (IPFS) cluster nodes. The primary goal of this research is to offer a layered architecture for the authentication and storage of medical devices that can prevent different security and privacy issues in IoMT-enabled healthcare. The suggested model is split into two sections: In order to protect the privacy of patient data, i) patient registration, ii) medical device authentication and authorization, and iii) information distribution in the blockchain network. The suggested paradigm resolves current issues and improves how the IoMT healthcare network operates. Distributed off-chain storage, which is highly secure and protects privacy, is the foundation upon which the paradigm is created and implemented. The suggested approach makes IoMT healthcare systems more scalable and enables secure access to patient data by utilizing an IPFS cluster. The solidity programming language (version 0.4.26) and the Remix IDE were used in the research. The IPFS cluster node, which it also immediately communicates with the application interface and guarantees device verification and the storing of their addresses is where the smart contracts are installed. The whole papers summarize in Table 3.

Table 3. Blockchain and IPFS-based MHR data authentication method

Papers	Techniques used	Advantages	Disadvantages	Implementations
[46]	The ciphertext policy attribute-based encryption system and IPFS storage environment, combined with blockchain technology	<ul style="list-style-type: none"> - Enabling the provision of secure sharing of medical images across domain networks. - Store user information on the blockchain ledger. - The authentication layer performs decryption and verifies the authenticity of the image. 	<ul style="list-style-type: none"> - Technologies for transferring medical images are inadequate owing to maintenance cost, privacy, storage, and security concerns. 	Theoretical research
[47]	Web App, Blockchain, IPFS	<ul style="list-style-type: none"> - Putting data in an IPFS hash for quicker retrieval that maintains duplicates everywhere to prevent a single point of failure. 	<ul style="list-style-type: none"> - Security and privacy of medical data - Performance - Scalability - Energy consumption 	Smart contract on a decentralized blockchain platform using Solidity.
[48]	Consortium blockchain network, IPFS	<ul style="list-style-type: none"> - Provides immutability and keeps privacy of the patient's records. 	<ul style="list-style-type: none"> - The model needs more numbers of peers and multiple sizes of megabytes of reports sharing system. 	Solidity
[49]	Blockchain, IPFS	<ul style="list-style-type: none"> - Protecting patient privacy, allows convenient access by approved authorities such as healthcare providers to medical data. 	<ul style="list-style-type: none"> - Misusing patient disease reports, unlawful access to medical records. 	Python
[50]	Smart contracts enabled consortium blockchain network, (IPFS) cluster node	<ul style="list-style-type: none"> - The decentralized nature of the system is guaranteed by the blockchain-based architecture. - For the patient and their medical devices, the registration-based security paradigm is described. - To maintain anonymity in the IoMT network, the access control is created and executed utilizing consortium blockchain. 	<ul style="list-style-type: none"> - Utilizing IPFS to create a distributed cluster - So much to process complexity is needed to maintain more devices in the system. 	Node js, solidity version 0.4.26 and remix IDE

5.4. Studies Discussion

According to the above studies, it is noted that Blockchain and IPFS are the best technologies to prevent and detect healthcare attacks. The main reason is that Blockchain and IPFS solutions are not centralized, therefore, there would be no copies of information that could be held for tamper. Also, Blockchain and IPFS cannot be changed; no one, not even the person in charge of the system, can change information written to a Blockchain and IPFS. As well as, there is a lot of discussion in the studies about the trade-off between the security objectives that blockchain and IPFS provide it and the cost, this is one of the important challenges. Finally, this integration between blockchain and IPFS is valuable and could implement in different situations in the healthcare environment.

6. A NEW MEDICAL HEALTH RECORD ARCHITECTURE MODEL BASED ON IPFS AND BLOCKCHAIN TECHNOLOGIES

The suggested system is divided into two modes, which include the entire process of storing and retrieving the medical health record utilizing the proposed decentralized system. Initially, in the first suggested mode is to encrypt the medical health record files to maintain data confidentiality. The system employs asymmetric or public-key encryption such as RSA, elliptic curve and others. After the encryption procedure is completed, the file will be uploaded to a distant or local IPFS node in the second stage. In turn, IPFS will hash the file using one of the hashing algorithms available, such as SHA-128, SHA-256, and so on, and then deliver the hash as a content identification. The system ensures data integrity in this stage since the content identifier functions as a unique identifier and any data alteration or manipulation results in the generation of a totally different content identifier. After signing the transaction using the user's blockchain wallet account, the system utilizes the smart contract to store the information on the blockchain in the later phases. Furthermore, the solution meets the requirement for data availability by making the information immutable on blockchain and IPFS. In the suggested mode, the system's goal is to save a few bits of information on the blockchain in order to reduce the cost and time necessary for storing actual files on the blockchain.

The second mode, which is retrieval of a medical health record, is split into three major parts. To begin, the user uses a smart contract to request a file or full list of the user's transactions (transactions including

the user's blockchain wallet address). The blockchain information returned is a particular transaction or a collection of transactions, each of which contains a set of information. The user will next use the hash of the necessary file to request the file from any IPFS node that contains the requested content identifier in the later stage. The IPFS node will then respond with an encrypted copy of the requested file. The relevant file will be on the user's device after completing the two preceding procedures. Finally, in order to view the file's contents, the user must decrypt it in the third step, as the file was encrypted when it was posted to IPFS using a one-time-use pair of public-private keys. As a result, and first and foremost, depending on who the user is (whether a patient or a hospital), the user's associated private key needs to be used to decrypt the created private key. The resulting private key will then be used to decode the requested file. Figure 4 depicts the entire model of the storing and retrieving processes.

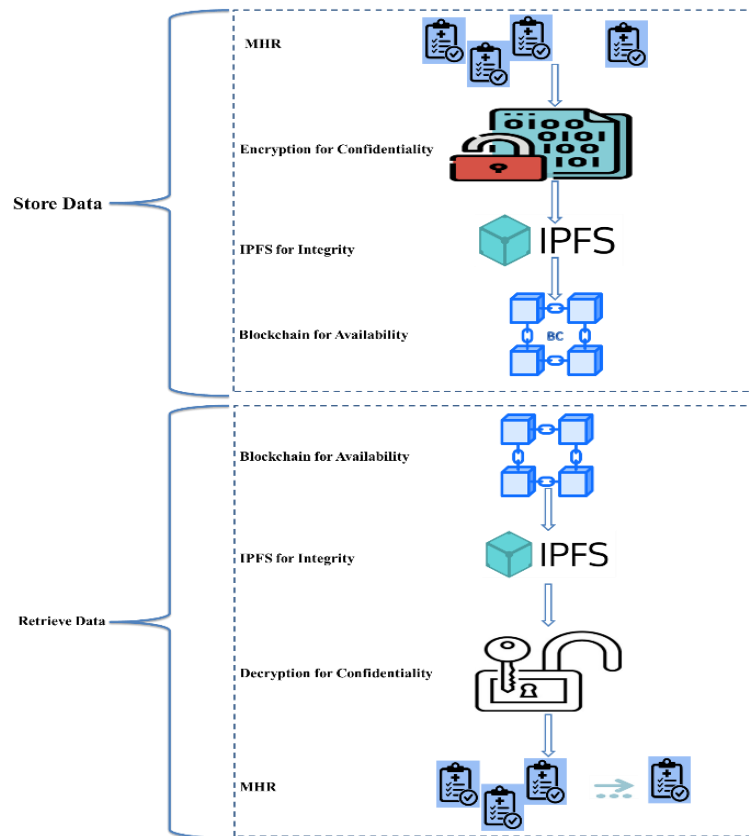


Figure 4. New medical health record data storage architecture model based on IPFS and blockchain technologies

7. CONCLUSION

After introducing these principles, this paper focuses on the implementation of IPFS and blockchain technology in medical health record data security. There are several apps available today for preserving the privacy of medical health records, achieving traceability of medical health record data, and confirming the integrity of medical health record data. However, there are several issues with these applications, some of which are design flaws and others of which are intrinsic issues with IPFS and blockchain technology. Future development should focus on improving the IPFS and blockchain-based system as well as the IPFS and blockchain technologies themselves, such as hash indexing, encryption algorithms, and consensus mechanisms. Finally, this article presents an IPFS and blockchain-based medical health record storage architectural paradigm.

REFERENCES




[1] Z. Wu, S. Xuan, J. Xie, C. Lin, and C. Lu, "How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective," *Computers in biology and medicine*, vol. 147, p. 105726, 2022. doi: 10.1016/j.combiomed.2022.105726.
 [2] S.-K. Kim and J.-H. Huh, "Artificial neural network blockchain techniques for healthcare system: focusing on the personal health records," *Electronics*, vol. 9, no. 5, p. 763, May 2020, doi: 10.3390/electronics9050763.

- [3] A. Mubashar *et al.*, "Storage and proximity management for centralized personal health records using an ipfs-based optimization algorithm," *Journal of Circuits, Systems and Computers*, vol. 31, no. 01, p. 2250010, 2022. doi: 10.1142/S0218126622500104.
- [4] A. A. Abdellatif *et al.*, "Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15762-15775, 2021. DOI: 10.1109/JIOT.2021.3052910.
- [5] M. Farahani and A. Shafiee, "Wound healing: From passive to smart dressings," *Advanced Healthcare Materials*, vol. 10, no. 16, p. 2100477, 2021. doi: 10.1002/adhm.202100477.
- [6] L. Meng and B. Sun, "Research on decentralized storage based on a blockchain," *Sustainability*, vol. 14, no. 20, p. 13060, 2022. doi: 10.3390/su142013060.
- [7] J. Odoom, X. Huang, and S. A. Danso, "COVID-19 and future pandemics: A blockchain-based privacy-aware secure borderless travel solution from electronic health records," *Software: Practice and Experience*, vol. 52, no. 10, pp. 2263-2287, 2022. doi: 10.1002/spe.3126.
- [8] G. Bigini, V. Freschi, and E. Lattanzi, "A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision," *Future Internet*, vol. 12, no. 12, p. 208, 2020.
- [9] 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, 2021, doi: 10.1002/spy2.162.
- [10] P. Prabha, Y. Janoria, H. Raj, U. Patidar, and K. Chatterjee, "medical image protection using blockchain for e-healthcare system," in *Smart Innovation, Systems and Technologies*, vol. 267, 2022, pp. 161-170.
- [11] M. Q. Alsudani, H. F. Fakhruideen, H. Abdul-Jaleel Al-Asady, and F. I. Jabbar, "Storage and encryption file authentication for cloud-based data retrieval," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 2, pp. 1110-1116, Apr. 2022, doi: 10.11591/eei.v11i2.3344.
- [12] 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, p. 974, May 2022, doi: 10.11591/ijeecs.v26.i2.pp974-988.
- [13] N. Nizamuddin, H. R. Hasan, and K. Salah, "IPFS-blockchain-based authenticity of online publications," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10974 LNCS, pp. 199-212, 2018, doi: 10.1007/978-3-319-94478-4_14.
- [14] A. Tenorio-Fornés, V. Jacynycz, D. Llop-Vila, 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-Janua, pp. 4635-4644, doi: 10.24251/HICSS.2019.560.
- [15] S. Wu and J. Du, "Electronic medical record security sharing model based on blockchain," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19*, 2019, pp. 13-17, doi: 10.1145/3309074.3309079.
- [16] G. Bigini, V. Freschi, and E. Lattanzi, "A review on blockchain for the internet of medical things: definitions, challenges, applications, and vision," *Future Internet*, vol. 12, no. 12, p. 208, Nov. 2020, doi: 10.3390/fi12120208.
- [17] P. A. Lobo and V. Sarasvathi, "Distributed file storage model using IPFS and blockchain," in *2021 2nd Global Conference for Advancement in Technology (GCAT)*, Oct. 2021, pp. 1-6, doi: 10.1109/GCAT52182.2021.9587537.
- [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. F. Fakhruideen, T. S. Mansour, F. I. Jabbar, and A. Alkhayyat, "Multiple inputs all-optical logic gates based on nanoring insulator-metal-insulator plasmonic waveguides," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 6, p. 6836, Dec. 2022, doi: 10.11591/ijece.v12i6.pp6836-6846.
- [20] M. K. Mohammed, A. A. Abdullah, and Z. A. Abod, "Securing medical records based on inter-planetary file system and blockchain," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 10, no. 2, p. 346, Apr. 2022, doi: 10.21533/pen.v10i2.2855.
- [21] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*. Cham: Springer International Publishing, 2019, doi: 10.1007/978-3-030-03035-3.
- [22] R. Mahzabin, F. H. Sifat, S. Anjum, A. A. Nayan, and M. G. Kibria, "Blockchain associated machine learning and IoT based hypoglycemia detection system with auto-injection feature," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 1, pp. 447-455, 2022, doi: 10.11591/ijeecs.v27.i1.pp447-455.
- [23] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Jul. 2018, vol. 2, pp. 359-364, doi: 10.1109/COMPSAC.2018.10258.
- [24] H. F. Fakhruideen, H. Abdul-Jaleel Al-Asady, T. Mahinroosta, F. Sohrabi, and S. M. Hamidi, "Novel add-drop filter based on serial and parallel photonic crystal ring resonators (PCRR)," *Journal of Optical Communications*, Dec. 2021, doi: 10.1515/joc-2021-0220.
- [25] Z. Kasiran, H. F. Ali, and N. M. Noor, "Time performance analysis of advanced encryption standard and data encryption standard in data security transaction," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2, p. 988, Nov. 2019, doi: 10.11591/ijeecs.v16.i2.pp988-994.
- [26] B. N. Alsunbuli, H. F. Fakhruideen, W. Ismail, and N. M. Mahyuddin, "Hybrid beamforming with relay and dual-base stations blockage mitigation in millimetre-wave 5G communication applied in (VIOT)," *Computers and Electrical Engineering*, vol. 100, p. 107953, May 2022, doi: 10.1016/j.compeleceng.2022.107953.
- [27] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications," *International Journal of e-Collaboration*, vol. 16, no. 1, pp. 16-32, Jan. 2020, doi: 10.4018/IJeC.2020010102.
- [28] S. Ghimire, J. Y. Choi, and B. Lee, "Using blockchain for improved video integrity verification," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 108-121, Jan. 2020, doi: 10.1109/TMM.2019.2925961.
- [29] P. W. Khan, Y. C. Byun, and N. Park, "A data verification system for cctv surveillance cameras using blockchain technology in smart cities," *Electronics (Switzerland)*, vol. 9, no. 3, 2020, doi: 10.3390/electronics9030484.
- [30] H. F. Fakhruideen and T. S. Mansour, "All-optical NOT gate based on nanoring silver-air plasmonic waveguide," *International Journal of Engineering and Technology*, vol. 7, no. 4, p. 2818, Oct. 2018, doi: 10.14419/ijet.v7i4.18955.
- [31] B. Singhal, G. Dhameja, and P. S. Panda, "How blockchain works," in *Beginning Blockchain*, Berkeley, CA: Apress, 2018, pp. 31-148.
- [32] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *Annals of Emerging Technologies in Computing*, vol. 2, no. 1, pp. 1-6, Jan. 2018, doi: 10.33166/AETiC.2018.01.001.




- [33] 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.
- [34] A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, and R. Jayaraman, "Blockchain-based multi-party authorization for accessing IPFS encrypted data," *IEEE Access*, vol. 8, pp. 196813–196825, 2020.
- [35] 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.
- [36] 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.
- [37] 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 & NETWORKS (COMSNETS)*, Jan. 2020, pp. 1–5, doi: 10.1109/COMSNETS48256.2020.9027313.
- [38] G. Subramanian and A. S. Thampy, "Implementation of blockchain consortium to prioritize diabetes patients' healthcare in pandemic situations," *IEEE Access*, vol. 9, pp. 162459–162475, 2021. DOI: 10.1109/ACCESS.2021.3132302.
- [39] M. Barati, W. J. Buchanan, O. Lo, and O. Rana, "A privacy-preserving platform for recording COVID-19 vaccine passports," arXiv, Dec. 2021, [Online]. Available: <http://arxiv.org/abs/2112.01815>.
- [40] N. Rauta and K. Shah, "Implementation of ethereum blockchain in healthcare using IPFS," *International Journal of Intelligent Communication, Computing and Networks*, vol. 2, no. 2, pp. 20–32, May 2021, doi: 10.51735/ijccn/001/17.
- [41] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Hyperledger healthchain: patient-centric IPFS-based storage of health records," *Electronics*, vol. 10, no. 23, p. 3003, 2021.
- [42] D. El Majdoubi, H. El Bakkali, and S. Sadki, "SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework," *Journal of Healthcare Engineering*, vol. 2021, 2021. doi: 10.1155/2021/4145512.
- [43] M. M. Sheeraz, M. A. Islam, and H.-C. Kim, "A decentralized approach of healthcare data collection for research," in *International Conference on Future Information and Communication Engineering*, 2022, vol. 13, no. 1, pp. 143–148.
- [44] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "BlockMedCare: A healthcare system based on IoT, blockchain and IPFS for data management security," *Egyptian Informatics Journal*, 2022.
- [45] M. Y. Jabarulla and H. N. Lee, "Blockchain-based distributed patient-centric image management system," *Applied Sciences (Switzerland)*, vol. 11, no. 1, pp. 1–20, Dec. 2021, doi: 10.3390/app11010196.
- [46] M. Y. Jabarulla, G. Jung, and H.-N. Lee, "Decentralized framework for medical images based on blockchain and interplanetary file system," *Conference Contribution*, 2019, doi: 10.6084/m9.figshare.14274941.
- [47] R. K. Marangappanavar and M. Kiran, "Inter-planetary file system enabled blockchain solution for securing healthcare records," in *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, Feb. 2020, pp. 171–178, doi: 10.1109/ISEA-ISAP49340.2020.235016.
- [48] R. Kumar and R. Tripathi, "A secure and distributed framework for sharing COVID-19 patient reports using consortium blockchain and IPFS," in *PDGC 2020 - 2020 6th International Conference on Parallel, Distributed and Grid Computing*, Nov. 2020, pp. 231–236, doi: 10.1109/PDGC50313.2020.9315755.
- [49] A. Al Mamun, M. U. F. 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*, vol. 1309, 2021, pp. 501–511.
- [50] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and IPFS technology," *The Journal of Supercomputing*, vol. 77, no. 8, pp. 7916–7955, Aug. 2021, doi: 10.1007/s11227-020-03570-x.

BIOGRAPHIES OF AUTHORS



Rana Abbas Al-Kaabi    received the B.Eng. degree in computer engineering from Imam Ja'afar Al-Sadiq University, Iraq, in 2018 and she is currently pursuing the M.S. degree in the Information Networks Department, College of Information Technology, University of Babylon, Iraq. Her research interests include, blockchain, smart contract, IPFS, security, and medical health system. As well as. She can be contacted at email: ranaa.net.msc@student.uobabylon.edu.iq.



Alharith A. Abdullah    received his B.S. degree in Electrical Engineering from Military Engineering College, Iraq, in 2000. MSc. degree in Computer Engineering from University of Technology, Iraq, in 2005, and his PhD. in Computer Engineering from Eastern Mediterranean University, Turkey, in 2015. His research interests include security, network security, cryptography, quantum computation, and quantum cryptography. He can be contacted at email: alharith@uobabylon.edu.iq.