RESEARCH PAPER

Blockchain Enabled Decentralized Application for Securing Electronic Medical Records with Smart Contracts

Akhila Thejaswi R[1], Permanki Guthu Rithesh Pakkala[1*], Bellipady Shamantha Rai[1], Sudheer Shetty[1], Vasudeva Rao P V[1], Srinidhi Rai[2]

[1]Sahyadri College of Engineering & Management, Mangaluru - 575007, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India

[2]Nitte (Deemed to be University), KS Hedge Medical Academy (KSHEMA), Professor and Head, Department of Biochemistry, Mangaluru – 575018, India

Received: *6th March 2026;* ***Revised:*** *18th April 2026;* ***Accepted:*** *8th June 2026;* ***Available Online:*** *11th June 2026*

ABSTRACT

Electronic Medical Records (EMRs) require a secure management system that preserves patient privacy and confidentiality while enabling authorized healthcare providers, such as physicians, to access medical information efficiently for clinical decision-making. Most of the health care systems use the traditional centralized database platforms for these data management; which is neither secure nor easy to maintain. These platforms can be replaced by distributed, efficient, and much more secure platforms which are backed by blockchain technology. In this work, a decentralized application (dApp) is developed which allows users to upload and download medical data to and from the distributed file storage system. The application's logic is written in solidity programming language in the smart contract. The application uses IPFS – Interplanetary File System, which is a distributed file storage system to store the medical records. Each file is broken down into pieces and each piece is given a hash which is stored on the blockchain. The user with right authentication has the privilege to access these hashes on the blockchain helping them in downloading the desired file. The application is tested through different nodes on the network which successfully resulted in securely storing and downloading the files from the distributed network. The dApp is tested with two performance metrics i.e. the number of transactions per unit time and the time taken to search records in the blockchain network. The results visualize that the data stored in the IPFS is immutable, distributed across its network which makes it impossible for anyone to just access it.

Keywords**:** Electronic Medical Records, Blockchain, Smart Contract, Decentralized Application, Interplanetary File System, Distributed File Storage System

How to cite this article: Thejaswi RA, Pakkala PGR, Rai BS, Shetty S, Rao PV, Rai S. Blockchain Enabled Decentralized Application for Securing Electronic Medical Records with Smart Contracts. Int J Drug Deliv Technol. 2026;16(6):825-835. DOI: 10.25258/ijddt.16.6.123

Source of support: Nil.

Conflict of interest: None

INTRODUCTION

The technological advancements in the healthcare sector can be utilized thoroughly only if diagnosis data of the patient data is available to all the practitioners whom the patient consults. In order to achieve this medical records have to be stored and preserved as electronic healthcare records and subsequently made available to all the authentic stakeholders[1]. Thus, currently blockchain enabled distributed databases are one viable solution to the efficient and storage of medical data with suitable access control mechanisms for authentic users [2, 3].

All block's in the blockchain contain a timestamp and a link to a previous block. Blockchains are highly resistant towards the tampering of the data[4].

Distributed Ledger: A blockchain uses Distributed Ledger Technology that can record transactions between two parties in an efficient and verifiable manner. Distributed ledger is a database that is consensually shared and synchronized across networks spread across multiple sites, institutions or geographies. All the transactions/contracts are maintained in decentralized form across different people and locations, which eliminate the need of a trusted third party. Every transaction should be accepted consensually by all the nodes on the network which makes illegal or unauthentic transactions rejected and tampering of the data on the blockchain near to impossible. Every transaction involves public "witnesses" which makes cyber-attack complicated. Each node has a participant who can access the recordings shared across that network and also owns a copy of it. By using different cryptographic keys and technologies, all the information in the blockchain is securely stored and accessed [5].

Ethereum and Smart Contract: Ethereum is a public, open-source software platform where decentralized applications can be built and deployed. Ethereum Virtual Machine (EVM) is a decentralized turing virtual machine, which uses a network of public nodes to execute scripts. Smart Contract is basically a piece of code which contains the business or the core logic of the application. In order to build blockchain applications, Ethereum is the go-to platform, as it gives the functionality to code smart contracts and deploy on the block. Once the smart contract is written and deployed to the main network it is not possible to change it later. Whenever a transaction happens, a smart contract computation is executed. It can be regarded as a stored procedure invoked upon a transaction[6]. Transactions resulted by calling functions of the smart contracts are agreed by every node. Blockchain in the field of healthcare/medical provides data privacy. Blockchain technology is used to verify a patient's health related data, record the history of prescriptions for future use etc.

IPFS: The traditional blockchain has the limitation in the uploading of a file to a maximum of 1 MB. In order to overcome this limitation, a distributed content addressable mechanism of file storage termed as IPFS (Inter Planetary File System) is now being employed. IPFS is a protocol used in peer to peer networking for the storage and retrieval of multimedia data in a distributed manner. The content address mechanism is used to access the stored data by peers in the network by making use of Distributed Hash Table.

Role of Cryptography in Blockchain:
Keys are used to validate and secure the transactions, where public keys are used to view the balance and transactions and the private key for authorization and authentication purposes. In order to have a successful transaction, a private key is needed to verify the ownership of an account. Hence every new transaction is added to the existing blockchain after being verified by all the nodes in the network. Private Key enables one way authentication, where a private key is required to unlock a participant's identity concerned with the blockchains information. Hashes are used to secure the chain of blocks in the blockchain. Blockchain technology preserves privacy of data such as personal information, or the information that are highly confidential by giving secured transactions[7].

Mining: Mining is the process of adding new transactions to the existing ledger of preceding transactions i.e. to the blockchain and also verifying the transactions on the blockchain network.

Role of Blockchain in Healthcare: Medical science has its own set of problems which reduce the effectiveness of the Healthcare system. Many of the problems relate to record keeping, data sharing and analyzing. Many applications of blockchain technology beyond crypto-currency relate strongly to record-keeping, existing standards on information and records management [8]. Blockchain in the field of health-care/medical provides data privacy. Blockchain technology is used to verify a patient's genetics data, identity or the history of prescriptions. Patients, doctors, anyone concerned with the healthcare field are the participants of blockchain network, where there is a secret private key and an open public key for every participant [9].

The major contributions in this work are:
Secure Medical Records Storage: The system uses IPFS for storing the medical records. The IPFS storage mechanism itself generates hash for the files to be stored thereby enhancing the security of the medical records.

Keyword based search: The medical records stored in the IPFS system can be searched by legitimate stakeholders with suitable access privileges. The record search time is estimated on varying amounts of loads.
Access Control: The concerned stakeholders with the private key only will be given access to the medical records.
Reduced record search time: The experiment results confirm that the developed Ethereum based dApp takes less time to search the medical records.
Increased transactions per unit time: The number transactions performed by the miners are increased with use of IPFS storage for medical records.

BACKGROUND

The areas related to the security and privacy aspects while using blockchain technology were dealt in many literatures in the recent past. Privacy mechanisms were discussed for non-anonymous users to carry out and publish transactions in Blockchain and making sure no other users can link to that transaction [10].

The scalability issues and the security issues faced while developing blockchain applications [11]. The technical challenges while using consensus algorithms such as Proof of Work are also examined. A Data Preservation system is developed using Blockchain which ensures that the data is not tampered or mishandled [12]. Also, cryptographic algorithm based data storage mechanisms are designed to ensure that data is encrypted. The performance evaluation metrics such as cost and response time is also very low.

A HAWK framework is developed using smart contacts for financial transactions[13]. The HAWK does not save the transaction in a blockchain thereby allowing privacy of transactional data. The main advantage of HAWK is that the cryptographic transactional protocols are automatically generated by the framework for developing smart contacts. In order to overcome the issues in blockchain such as heavyweight increased distributed ledger size, time consuming data synchronization, and lightweight master-slave blockchain architecture [14].

There is also specific research going on with securing and preserving privacy of patient's medical records. Technical solutions were deliberated to solve the issues pertaining to storage, management and securing the medical records in an efficient manner.

The blockchain technology has many advantages in the healthcare sector[15]. The tradeoffs between the database systems and blockchain technology is discussed. A framework BLOCKBENCH is designed to evaluate the workloads of processing the data. The blockchain technology is applied to healthcare applications based on the features of distributed ledger such as decentralized management of data, robustness, availability, consensus protocol, security and privacy are deliberated [16].

A mechanism is devised to avoid loss of health records data which would hamper the privacy of patient a Blockchain enabled smart-contract for Ethreum is developed, which makes use of cryptographic encryption to search the data blocks and also is enabled with complex logic expressions for the purpose of data indexing. Data indexing over here ensures that only index values are propagated in a blockchain transaction and hence complete control over the data is at the user's side[17].

The health care sector has induced technologies such as Cloud to store the health record to ensure the availability of the data. In this work, authors have discussed the usage of Blockchain in the cloud data of health records to ensure the security and privacy aspects[18]. The main advantages of using Blockchain in maintaining Health records are:

- No trusted third party is required
- Patients can be given the access permission to control the data
- The health history can be easily viewed from anywhere in a timely, complete, accurate way.The main challenges of blockchain in health data are:
- Typically blockchains were used for small transactional data unlike the size and volume of health records which are relatively large.
- The immutability feature of blockchain does not permit alteration of data once uploaded.

A Health Care Data Gateway (HDG) is proposed, where all the private health information of a patient is controlled by himself [19]. HDG also utilizes a

database schema which tabulates health care data for practical ease of usage. The application ensures that an un-trusted third party may use the data for computations under the privacy norms. The e-health records maintained via blockchain technology can be used for data analysis and research maintaining privacy aspects of the data [20]. The structured e-health records may also be exchanged by particular patients for crypto currencies.With usage of Blockchain, the health records can be maintained individually by patients itself who can grant and rescind the access control to other parties.

The health records are currently stored in different database servers of different hospitals, thereby making it difficult to culminate data of a single patient and draw suitable conclusions. Also, there are no suitable data sharing policies for e-health informatics which is one of the hurdles in developing appropriate medicines and vaccines. To overcome these issues Medblock a Blockchain technology to access and retrieve e-health records is created. Medblock provides security through access control mechanisms based on hashing technique and asymmetric cryptography.

A data management system is developed for health records termed Medrec are created which gives easy access to patients [21]. Medrec has blockchain properties such as authentication, confidentiality and data sharing. This blockchain allows all the medical stakeholders to fit in and access the data in a controlled manner. The smart contracts have developed which initiate an action imitated by the user of blockchain[22]. The data is shared between the cloud service providers and the blockchain users in an efficient manner using access control protocols.

Ancile - a blockchain is developed which focuses on preserving privacy of Electronic Health Records is developed [23]. The developed system uses hashes of data to transmit the data sought by the user, over an HTTPS protocol. The approach also uses permissioned blockchain which makes validation of nodes easier. A blockchain technology is developed to secure health records using attribute-based cryptosystems [24]. The medical data encryption is done using attribute based encryption and identity based encryption. The identity based digital signatures are used to verify the integrity of the hashes of the data records.

MATERIALS AND METHOD

The architecture diagram of the Medical Data Storing Blockchain application is depicted in Figure 1. The architecture shows us that there are two functionalities i.e.; uploading the file to the IPFS, and storing the returned hash from the IPFS on to the blockchain and downloading the file using the hash from the blockchain. IPFS is used here since it is the best distributed file storage system available in the market. IPFS lets us address large amounts of data and place the immutable, permanent links into blockchain transactions. This timestamps and secures content without having to put the data itself on the chain.

The application uses RSA encryption algorithm to encrypt the files before they are uploaded to the IPFS. As IPFS uses the SHA-256 hashing algorithm it generates a unique 32-byte hash for the encrypted file uploaded. It also uses node.js runtime environment for JavaScript at the backend of the application to access the routes.

The application has the following components:

1. The web application's User Interface is a simple frontend containing HTML and CSS.
2. The UI part of the application allows the user to upload the file to the IPFS and download the file using the hash.

The following steps illustrates the file uploading process as depicted in Fig. 2:

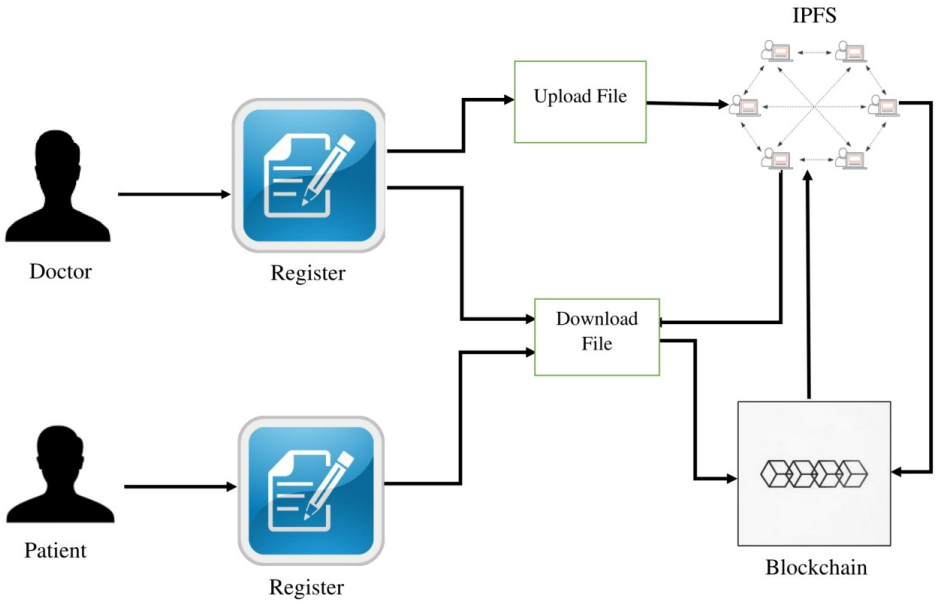

Figure 1: Architecture Diagram of Medical Data Storing Blockchain Application

- File consists of patient health records. These records may include diagnosis report, X-ray, scanning reports etc. of the patient. Records may be in the format of text, images, and video. The file to be uploaded is selected from the system of the user.
- The selected file containing the medical data is given as an input which results in delivering the IPFS hash of the file uploaded as the output.
- The file uploaded by the user is encrypted using RSA encryption algorithm for enhanced security. The process of encryption is executed using a public encryption key.
- After the file is encrypted, the file is uploaded to the IPFS. It produces a cryptographic hash of the file stored in it. IPFS uses SHA-256 algorithm.
- Hash of the file produced by IPFS is 32 bits in length.
- A block is created containing a hash of the file stored in IPFS, hash of preceding block and timestamp. Blockchain also uses SHA-256 hash algorithm for finding hash of each block.
- This block creation is achieved by invoking the function logic defined in the smart contract.
- Once the block is created, the block is added to the chain of blocks. Each block contains a hash of each file stored in the IPFS.
- After appending the block to blockchain, the hash of the block is made available to the users.
- The user who has uploaded the file can grant permission to the user who has requested to access the file.

The pseudo code for file upload is shown below:

```
FUNCTION: file upload
INPUT: patient record file
OUTPUT: IPFS file hash
BEGIN
 initialize ipfs <- ipfsAPI("ipfs.infura.io", "5001",
{ protocol: "https" })
 upLoad file(file, fileDescription):
   fetch user, fetch users
   initialize empty array chuncks
   initialize encryptionSize <- 256
   FOR i=0; i< file.data.length ; encryptionSize ++:
    let publicKey equal to find user.adhaarNumber
== fileDescription.permission of public key
   IF value == true:
    let chunk <- data.slice(i, i + encryptionSize)
    let encryptedData <-
crypto.publicEncrypt(publicKey, chunk)
    output "file encrypted"
    append encryptedData -> array chunks
    let data <- await
ipfs.files.add(Buffer.from(chunks))
```

```
output "file uploaded to ipfs"
let hash <- first element of data array
FOR file in files:
 IF file.hash == hash in files:
  return
 ELSE:
  fileDescription.name <- file.name
  fileDescription.mimetype <- file.mimetype
  fileDescription.hash <- hash
  fileDescription.date <- Date.now()
  fileDescription.size <- file.length
  push fileDescription to files
 ELSE:
  return
END
```

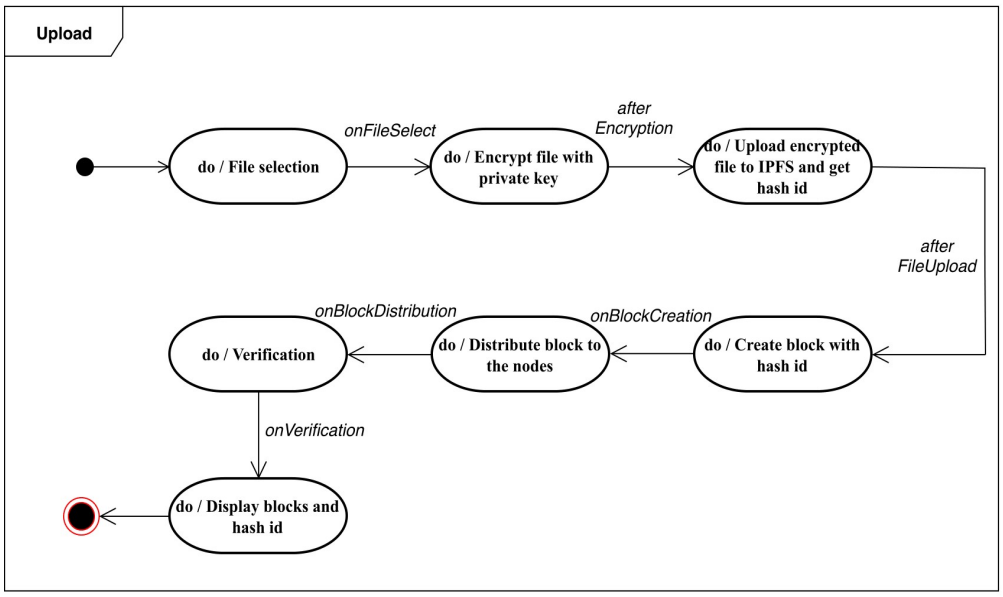

Figure 2: State Diagram for Uploading the File

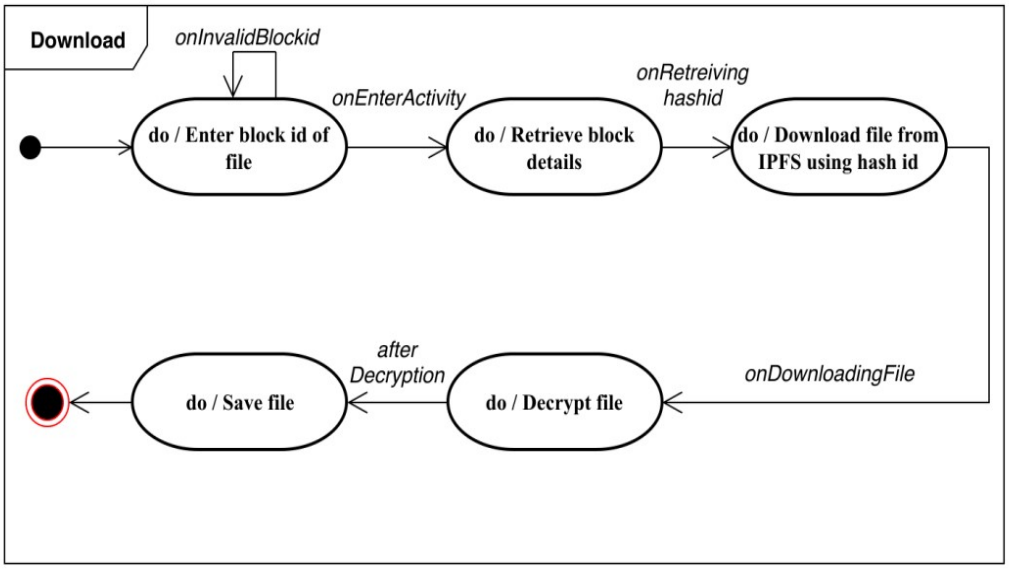

Figure 3: State Diagram for Downloading the File

The following steps illustrates file downloading process as depicted in Figure 3:

- This functionality takes input as the hash of the block and outputs the file containing the patient's data.
- Search for the owner of the file which needs to be accessed using the unique id of the user. Identify the file that has to be downloaded from the list of file hashes of the user.
- The required file can be downloaded by clicking on download option. Followed by this step will be two scenarios:
    a. If permission is granted to access the file - Identify the block in the blockchain using its hash, retrieve the IPFS hash of the file from block, Download the encrypted file, Decrypt the encrypted file and save the file in the system.
    b. If permission is not granted - Identify the block in the blockchain using its hash, Request to access the file which is basically sending a request to the owner to get the file's access. If a request is accepted and permission is granted, return to scenario a.

The pseudo code for downloading the file is shown below:

FUNCTION: download file
INPUT: IPFS file hash
OUTPUT: patient record file
BEGIN

```
 ipfs <- ipfsAPI("ipfs.infura.io", "5001",{ protocol: "https" })
 downloadfile(hash):
   user <- fetchuser()
   initialize empty array chunks
   initialize encryptionSize <- 256 * 2
   initialize file
   initialize decrypted
   file <- await ipfs.files.get(hash))[0]
   output "file downloaded from IPFS"
   FOR i = 0; i < file.content.length; i = i + decryptSize:
     chunk <- file.content.slice(i, i + decryptSize)
     decrypted <- crypto.privateDecrypt({key: user.privateKey,passphrase: user.aadharNumber},chunk)
     push decrypted to chunks
     output "file decrypted"
     return buffer from chunks
```

END

IMPLEMENTATION DETAILS

The dApp application runs on point to point networked systems. Its architecture consists of the Ethereum virtual machine containing the blocks and the smart contract deployed to blockchain and which resides on one of the blocks, web3 provider, metamask browser extension, web3.js API services serving the HTML, CSS, and JavaScript on the client's browser. The dAPP is implemented using the technical specification available in Table 1.

Table 1: Technical Specifications of the System Developed

Parameter	**Value**
Processor	Intel(R)core(TM)i7-9600 CPU@3.00 GHz
Memory	8 GB
Operating System	Windows 10 Pro
Programming Language	Solidity

As the user uploads the file to the system, the file is encrypted and uploaded to the IPFS. A block for the file is created with an IPFS hash and added to the Blockchain. Thus, no other intruder can access the files without the permission of the user. Even though some third-party entity manages to change the contents of the file, that results in the change in the hash value which will not match exactly to that of the hash on the blockchain. Since each of the blocks on the blockchain contains a cryptographic hash of the preceding block, none of the blocks containing files related data can be tampered. Thus, keeping all files secure in a distributed ledger.

Figure 4 shows the blocks of the blockchain containing the details of the files uploaded to the IPFS. Each block contains the hash, author information, and the information of the users to whom the file access is permitted, size of the file, title of the file and description of the patient record. After every file gets uploaded and its hash gets stored on the blockchain, a new block is created and gets appended to the existing chain.

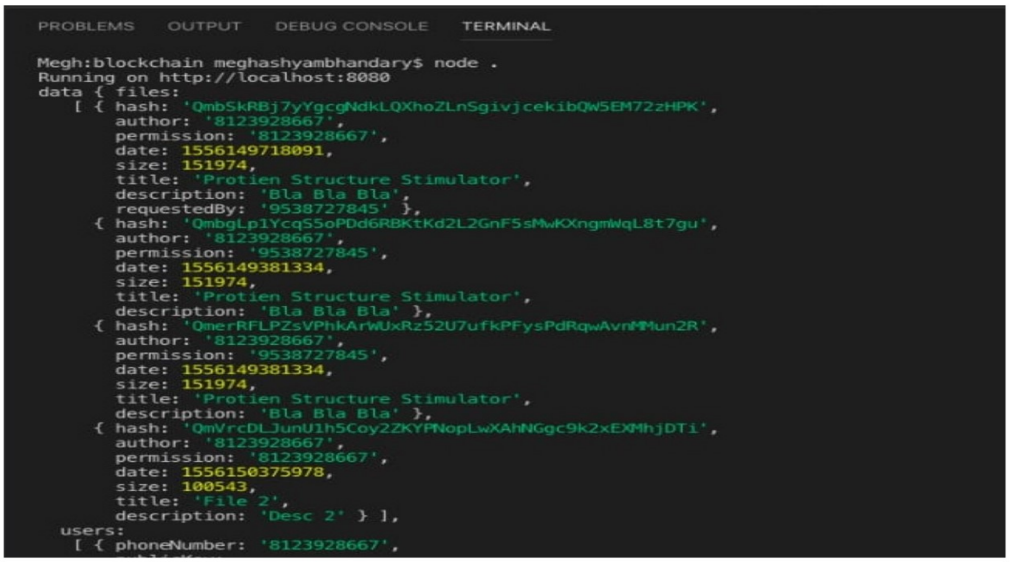

Figure 4: Implementation of Chain of Blocks

Filename	Description	Hash	Size	Date	Action
Protien Structure Stimulator	Health	QmbSkRBj7yYgcgNdkLQXhoZLnSgivjcekibQW5EM72zHPK	151974 bytes	Thu Apr 25 2019 05:13:01 GMT+0530 (India Standard Time)	Ask Permission
File 2	Desc 2	QmVrcDLJunU1h5Coy2ZKYPNopLwXAhNGgc9k2xEXMhjDTi	100543 bytes	Thu Apr 25 2019 05:29:35 GMT+0530 (India Standard Time)	Ask Permission

Figure 5: Ask Permission to Download

Filename	Description	Author	Hash	Size	Date	Requested by	Action
Protien Structure Stimulator	Health	8123928667	QmbSkRBj7yYgcgNdkLQXhoZLnSgivjcekibQW5EM72zHPK	151974 bytes	Thu Apr 25 2019 05:18:38 GMT+0530 (India Standard Time)	9538727845	DownloadGrant

Figure 6: Grant Permission to Download

Figure 5 shows the list of files a user has uploaded and another user can ask permission with the owner of the file to access and download the file. Once the user asks permission, the owner of the file receives a request.

Figure 6 shows the list of requests the user has received. The user then decides on whether to grant permission or not. After the permission is granted, the user who requested the file can download the file.

RESULTS AND DISCUSSION

The medical health records are run through a TestRpc environment which is available in the Ethereum environment. Using TestRpc we can simulate the Ethereum environment on the client side locally.

The following parameters are used for the experimentation:

- **Hash Rate:** It is the unit of processing a hash operation per unit time for a block. The higher the hash rate the better will be the mining capacity.
- **Network Hash Rate:** It defines the hash rate of the blockchain network.
- **Block Time:** The average time required to add a new block into the blockchain network.

The parameter settings for the simulation are mentioned in Table 2:

Table 2: Parameter Setting Values for Etherem Environment

Parameter	Value
Hash Rate	25 MH/s
Network Hash Rate	240314.96 GH/s
Power	125 watts
Block Time	14.4 s

Table 3 indicates the total number of transactions that are mined and the time it takes to mine. The numbers of transactions are varied from 50 to 1000, and the estimated time in seconds is observed and tabulated. Since the medical records include multimedia files the transaction time is high and varying.

Table 3. Transactions Mined versus Time Taken

No. of Transactions	Time (Sec)
50	6
100	10.6
200	16.3
500	34.5
750	56.8
1000	66.7

In Table 4, the time taken to search the medical record is tabulated. It is inferred from Table 3 that when the search for medical records are increased the time taken to search the record does not increase proportionately. This is mainly due to the fact that the medical records are linked as blocks in

the blockchain. Thus the dApp system developed using IPFS provides time efficiency as compared to general cloud storage based blockchains.

Table 4: Time Taken to Search Medical Health Records

Total Number of Records	Time (ms)
1	0.12
5	0.78
10	1.43
20	1.94
30	2.27
40	2.45
50	2.67

Even Though the developed system gives time efficiency in transaction mining and searching of the records however there will be load on the storage because of the size of the multimedia images which the miners will have to bear when there is a need to keep the copy of medical records in the distributed blocks.

CONCLUSION

In this work, the proposed application dApp illustrated how blockchain and the distributed ledger technology can help improve data management in the health sector which is very essential. However, this application allows a user to upload the encrypted files to the IPFS such that it is very safe and tamper proof and the hashes of the files are recorded on the blockchain which guarantees that any changes made to the file will change the hash value thus bringing out the attention to the user. The performance metrics such as the number of transactions per unit time and the time taken to search the multimedia medical records is compared and it is observed that the time taken reduces with the number of records. The result shows that the execution time increases as the number of transactions increases, indicating a positive correlation between workload and processing time. The growth is approximately linear, with a steeper increase between 500 and 750 transactions, followed by a more moderate increase up to 1000 transactions. This trend suggests that the system scales reasonably well while maintaining predictable performance as transaction volume grows.

One of the major challenges of the proposed work is achieving transaction scalability comparable to centralized payment systems such as Visa and Maestro, which are capable of processing a significantly higher volume of transactions with low latency.

REFERENCES

1. Devi GD, Tamilpavai G. Securing electronic health records using blockchain-based bi-layer algorithm with bit swapping codon encryption. Biomedical Signal Processing and Control. 2026 Apr 15;115:109314.
2. Ge S, Meng H, Khan S, Alhayan F. A Blockchain-Based Smart Contract Framework for Autonomous Sports Training Management in Multi-Agent Environment. Transactions on Emerging Telecommunications Technologies. 2026 Feb;37(2):e70364.

3. Kumar MK, Borole YD, Mallick S, Chaba Y, Kumar S, Khan S, Alhayan F, Shavkatov N, Gupta R. Blockchain-Enabled Privacy-Preserving Anomaly Detection and Reputation Framework for VANETs. Transactions on Emerging Telecommunications Technologies. 2025 Nov;36(11):e70290.
4. Premila Rosy C, Sithar Selvam PM, Priya T, Kumar M, Khan S, Mayakannan S. Decentralized Secure Computation Offloading for Mobile IoT Devices Using Blockchain and Metaheuristics. InNext-Generation Computational Intelligence: Trends and Technologies 2025 Oct 1 (pp. 283-301). Cham: Springer Nature Switzerland.
5. Nekouie A, Vafaei Jahan M, Moattar MH, Sheibani R. Secure electronic health record access control via blockchain, dual-attribute encryption, and large language model-based attribute extraction. Scientific Reports. 2026 Feb 17;16(1):8673.
6. Segar N, Vijayan V. SENTINEL-Chain: a blockchain-integrated privacy-preserving framework for secure healthcare data publishing. Frontiers in Digital Health. 2026 Jun 9;8:1807540.
7. Singh N, Panigrahi R, Panigrahi RR, Meher JR. Unraveling blockchain adoption in the insurance sector: a comprehensive TOE framework with knowledge management practices. VINE Journal of Information and Knowledge Management Systems. 2025 Aug 26;55(5):1251-71.
8. Mallick SR, Sobhanayak S, Lenkar RK. Secure and trusted data sharing in smart healthcare using blockchain and IoT integration. Discover Internet of Things. 2025 Aug 19;5(1):90.
9. Albanese G, Calbimonte JP, Schumacher M, Calvaresi D. Dynamic consent management for clinical trials via private blockchain technology. Journal of ambient intelligence and humanized computing. 2020.
10. Henry R, Herzberg A, Kate A. Blockchain access privacy: Challenges and directions. IEEE Security & Privacy. 2018 Aug 6;16(4):38-45.
11. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In2017 IEEE international congress on big data (BigData congress) 2017 Jun 25 (pp. 557-564). IEEE.
12. Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-based data preservation system for medical data. Journal of medical systems. 2018 Aug;42(8):141.
13. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In2016 IEEE symposium on security and privacy (SP) 2016 May 22 (pp. 839-858). IEEE.
14. Ma Z, Huang W, Bi W, Gao H, Wang Z. A master-slave blockchain paradigm and application in digital rights management. China Communications. 2018 Aug 16;15(8):174-88.
15. Pirtle C, Ehrenfeld J. Blockchain for healthcare: The next generation of medical records?. Journal of Medical Systems. 2018 Sep;42(9):172.
16. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017 Nov 1;24(6):1211-20.
17. Lee E, Yoon Y. Trusted information project platform based on blockchain for sharing strategy. Journal of Ambient Intelligence and Humanized Computing. 2022 Mar 1;13(3):1575-85.
18. Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future generation computer systems. 2020 Jun 1;107:841-53.
19. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems. 2016 Oct;40(10):218.
20. Hoy MB. An introduction to the blockchain and its implications for libraries and medicine. Medical reference services quarterly. 2017 Jul 3;36(3):273-9.
21. Khatoon A. A blockchain-based smart contract system for healthcare management. Electronics. 2020 Jan 3;9(1):94.
22. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via

blockchain. IEEE access. 2017 Jul 24;5:14757-67.

23. McGhin T, Choo KK, Liu CZ, He D. Blockchain in healthcare applications: Research challenges and opportunities. Journal of network and computer applications. 2019 Jun 1;135:62-75.

24. Wang H, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of medical systems. 2018 Aug;42(8):152.