2021 2nd Global Conference for Advancement in Technology (GCAT)
Bangalore, India. Oct 1-3, 2021

Distributed File Storage Model using IPFS and Blockchain

Pearl Alisha Lobo
Computer Science & Engineering
PES University, Bangalore,
India, 560100
Email: plobo3270@gmail.com

Sarasvathi V
Computer Science & Engineering
PES University, Bangalore,
India, 560100
Email: sarsvathiv@pes.edu

2021 2nd Global Conference for Advancement in Technology (GCAT) | 978-1-6654-1836-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/GCAT52182.2021.9587537

***Abstract*— In current scenario the patients' medical report is stored digitally in medical industry. The report consists of patients' details such as patients' private details, medical reports, and doctor prescriptions. This sensitive information is stored in centralized storage model. The disadvantage of this system is that there is problem in safeguarding user's security. The problems such as illegal access of private data such as identity data and illness of the patient, and their medical reports. To address this issue, distributed file system of medical data using Interplanetary File System and blockchain technology is proposed. Where hash value of the report is stored in blockchain thus reducing the size of blockchain and the file is stored in IPFS. In IPFS the file is stored as hash value of the file. This framework preserves patient privacy and facilitates easy access of details of patients by authorized users such as doctors and patients. From this framework availability, integrity and consistency was achieved.**

Keywords—IPFS, Blockchain, SHA-256.

I. INTRODUCTION

The medical field produces large amount of medical data that needs to be stored, distributed, and accessed regularly. It is produced when a patient goes through a medical check-up such as computerized tomography, ultrasound diagnosis, and X-Ray. When a specialist gives a prescription, the data is created that should be saved and accessed by health providers whenever there is availability for the medical data. The health providers from other hospitals should have access for the medical data. However, the data should be kept private and should be immutable. The medical record is stored as transparent process, as it demands a system where data can be easily accessed and maintained regularly. In recent world, there are several distributed file storage systems streaming everywhere on the world. The issue of unwanted space and access to different peers in the system arises in these applications. BitTorrent is the distributed file storage system and sharing application which includes untrusted peers. The most important thing is that millions of users utilize BitTorrent consistently. But the drawback of BitTorrent is security. HTTP convention is one of the most significant convention regarding improvement for conveyed applications around the world it chips away at location addressed based conventions which isn't much efficient. Because HTTP works as per client-server model, so if the server is down or there is heavy traffic on server the client may not be able to reach the server. To solve the issue of BitTorrent and HTTP, distributed file storage network is used. The IPFS uses the content-addressed technique to store and access the file rather than location-based address. The structure is designed in such a way that data is distributed on different nodes to provide distributed storage system and each node in the network is a peer to another node. All the peers have same potential to share and retrieve the data that is no node is master to other node.The network stores the copies of data in other nodes which guarantees the accessibility of data in the framework. IPFS is a distributed file capacity framework which is P2P network, it computes the hash value of a file while storing the file. All the peers in the network will have access to the hash value of the files. The new hash value is created if the file is edited and not the original file or hash is altered. IPFS encourage the Distributed Hash Table (DHT) which is a lot better than BitTorrent, and Git file capacity framework. IPFS is called version-controlled framework which guarantee the security, reliability, and scalability which are missing in current distributed file systems. The blockchain innovation is a decentralized system, where a user's clinical record can be shared effectively among the companions (clinics or specialists) in a medical services framework. Consistency, immutability, privacy and integrity are the features of this technology which are required in medical industry. The blockchain comprises of a set of transactions which are connected with the assistance of hash and assures the immutability of the transactions (medical records). The medical data of the patient can be stored in blockchain network and distributed among peers efficiently in blockchain. Every record in the blockchain is structured in such a way that it is permanent and not tampered and is easily accessible by the users. Thus, to manage large amount of medical data, distributed storage system with a peer-to-peer network is required. Interplanetary File System (IPFS) provides a peer-to-peer (P2P) distributed storage system where large amount of data can be stored effortlessly. In IPFS file is stored as content addressed hash rather than location-based address. The content-addressed hash is stored in a distributed hash table (DHT). IPFS has a version control system wherein each report is matched with its hash an incentive in DHT. It removes duplicate copies of files using version-control history. IPFS stores the document as hash of records to ensure quick request access time. To get to a patient's clinical report, a companion can utilize the relating hash estimation of the report.

A. Blockchain

Blockchain Technology is a system of continuously growing list of records without tampering or revision of records. Blockchain is a chain of blocks of data or digital information. In the Fig.1, every block of the blockchain has hash of previous block, root hash, nounce value and timestamp. Nounce value is a counter value used for proof of work. Timestamp is the time at which the block was created.

A block is created when a sender initiates the transaction process. The new block is verified by all the nodes only then it is added to the chain. During the verification process the transaction is included to the set of unconfirmed transaction. The miner picks one transaction at a time from the pool of transactions to create a block. Once the miner picks the transaction then tries to add his proof of work to the block. Proof of work a mathematical puzzle that should be decoded by the miner. Every new transaction will be having a new puzzle that should be decoded by miner. That is each transaction will have one puzzle that will be broadcasted to all the nodes. So, the first node who solves the puzzle will add his proof of work to the block. Once the block is created it will broadcast the nounce value, block value to all the nodes. The verifying miners will receive nounce value, new block to verify. The other miners will apply hash function to the received block and then match the value with received hash value. If it is successful then miners will give their confirmation to add the block to blockchain.

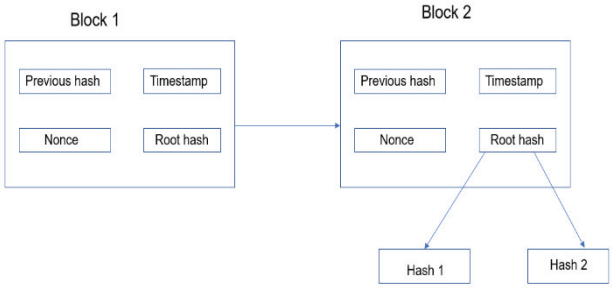

Fig. 1. Blockchain – IPFS node

B. IPFS

IPFS stands for Interplanetary File System that is peer-to peer distributed system. It is versioned file system that can take files and manage them and store them and then track versions over time. IPFS uses peer-to peer system i.e here every node is client and server and connected via internet. When the client needs to download a file, it will download small chunks of the file from multiple other peers simultaneously combining them locally to recreate the entire file. This speeds up the downloading time. It uses content-address system by applying hash function which is used as the address of the file rather than location-based address. The hash value represents root hash of the file i.e content-address of the file. When the file is added to IPFS the raw data is chunked into 256K size of chunks. Then each chunk is hashed by SHA-256 hash function and hash value is created for each chunk. The hierarchical data structure is created by combining all the calculated hash value for which a single root hash is computed. The data structure used is Merkle DAG. So, when requesting server for the file we can access to the starting point of data.

II. Literature Survey

Blockchain is a model that coordinates decentralized storage model. Blockchain is used to record the patients report in recent days for achieving security to the report and. The information in blockchain is consistent, therefore the information will not be altered. Blockchain can be considered as a additional protective layer that can prevent malicious activities in the field of computer technology by acting as a protective layer for user's data against the attackers [12]. The IPFS is a decentralized storage model. It shares and stores all kinds of files. It creates a specific hash value for each file based on the file content. In addition, IPFS has a deduplication mechanism, which can adequately try not to rehash storage of information and recoveries the extra room. IPFS stores medical records. The blockchain creates a distributed access and validation system to completely replace the current centralized intermediaries [1]. The document is pushed to the IPFS network through TCP attachment. Furthermore, the document is added to the Ethereum Blockchain. At the point when the document is requested by the client from the organization, the record trustworthiness should be checked by recovering from the Blockchain. The access time to fetch data from IPFS may vary since it is fetched from cloud [13]. This approves the respectability of the document. The hyper ledger fabric gives a path which can be utilized as proof for both scientific examination and debate goal [2]. On the off chance that somebody takes a record off IPFS and illicitly shares it with others it will distinguish who has downloaded the file. Hyperledger fabric is a permissioned blockchain innovation which is a private blockchain. Every node in the blockchain is known to one another and individuals are consents to join. The blockchain is answerable for dealing with the metadata of the document framework and blockchain record just stores the exchanges related metadata. This will bring about high storage since we guarantee measure of metadata is a lot smaller than the raw information. Hyper-IoT is a decentralized, distributed, private blockchain network that works on Hyperledger Fabric framework. The private sub network can be created per confidential domain using Fabric organizations and channels where only authorized users subscribe to, thus restricting access to data [11]. Block stack is a worldwide naming and capacity framework made sure about blockchain [3]. Block stack is delivered as open-source software. Zig-Zag codes are eradication codes which is normally partition the first document. Block stack has four layers two layers in control and other two for information. Initial two layers are for confirming the legality of the exchange. These two layers contains blockchain and virtual chain layer. Each record is developed to incorporate a mark from the senders' private key. In this way, the node that gets the record checks the uniqueness of the mark through the record's senders' public key. Other two layers are routing and storage layer. Routing layer holds data of the routing address of each record and their documents under this record. In storage layer the information is divided into hot information and cold information. Hot information is regularly utilized information and cold information is rarely utilized information. For hot information triple replication conspire and for cold information deletion codes stockpiling plan is applied. IPFS based blockchain information storage model is the place where it transfers the document to IPFS organization and afterward restores the hash of exchange and that hash is put in blockchain [4]. The blockchain information is largely diminished. IPFS utilizes content address to get the record from file system. Content address has the hash of the record instead of the document. For adding the block to the blockchain two work processes are followed to be joining the network cycle and the mining cycle [5]. At the point when new node joins the organization, it will request with the neighboring nodes to acquire blockchain record. It will make neighborhood record i.e information base that stores the metadata of blocks and the log. The recently node joins the network and is synchronized.

Decentralized Applications use decentralized EVM, and its smart contracts. The cost of server-side hardware is reduced by using distributed storage. And availability data is improved [9]. The crowdfunding using Blockchain works as decentralized system where no platform control the smart contracts. A smart contract is a collection of code deployed using cryptographically signed transactions on the blockchain network. The smart contract is executed by the nodes within the blockchain network; all nodes must derive the same results for the execution and results of execution are recorded on the blockchain [15]. A consensus protocol is used for transaction and communication between nodes [13]. It works on peer to peer network and inter-node communication protocol to verify new block. The modification of any block is not possible.[10].

III. Proposed Model

The system that is planned to be modelled is to upload the file, encrypt the file, store the encrypted file in IPFS, store the transaction in blockchain and retrieve the file when requested. There includes four main entities in this system design, namely Blockchain, IPFS, Server, and User. The data generated by the system will be stored in the IPFS while ensuring its consistency, integrity, and availability as shown in Fig. 2.

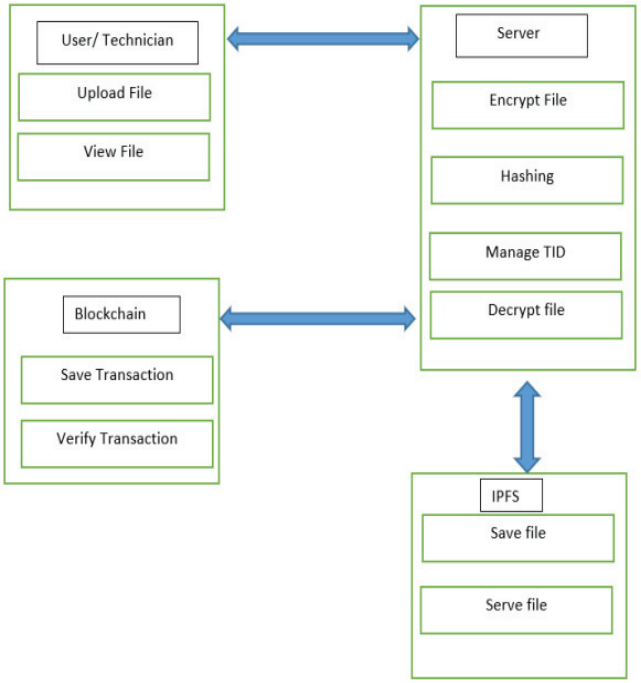

Fig. 2. Architecture Diagram

A. Blockchain

Blockchain innovation is a decentralized framework, a constantly growing list of records without the chance of altering and correction. Every node of the organization stores the whole record information in the blockchain. Thus, the blockchain instrument varies totally from DHT, where the information is dispersed between hubs. Each exchange to the blockchain should be approved by the miners by the process called mining. The blockchain can save the data provided by the user, and provide data when requested by the user. The data contains patient id, hash value of the file and the transaction id fetched from the IPFS. When a user requests for a file, the server will fetch the data from blockchain to verify the file.

B. IPFS

IPFS is a distribued file framework which is P2P network. The IPFS computes the hash of a file while storing the file and that hash value is available to all nodes. The new value is created if the file is altered in the file. And not the original file or hash is altered. IPFS uses distributed hash table (DHT) and called as version controlled system. IPFS can save the file provided by the user, and provide file when requested by the user. The file is uploaded as chunks of a file and will create a directed acyclic graph and store the hash of chunks of the file. When the user requests for a file the IPFS returns the chunks of the file to the user.

C. Server

The server includes users such as doctors, technician and patients. The server is able to encrypt the file and upload to the IPFS. For every upload to the IPFS a transaction id is created. The server is able to retrieve the id. The server generates the hash value of the file. The server creates the transaction id which contains patient id, hash value and the retrieved transaction id from the IPFS. The server will upload the transaction id to the blockchain. When the user requests for file the server will fetch the file from IPFS, apply hash function to the file, verify it with stored hash in blockchain and decrypt the file.

D. User

The users contain doctors, technician, patients. The doctor and the technician can upload the file. The patient and doctor can view the file. Each user will be having a unique id which can be used to login to the system. Before Uploading, the file is encrypted using patient id as the encryption key and AES symmetric algorithm is used. The doctor and patient can request the file to be viewed and is requested as a hash of the file by the user. The user can view the file if only the hash of the encrypted file retrived from blockchain and generated hash of the encrypted file fetched from the IPFS matches. Then the file is decrypted and user can view the file.

The user uploads the file to IPFS. Before uploading the file it will be encrypted by the server using AES symmetric encryption and patient id as the key for encryption. The IPFS stores the files as hash value of the file. For every file stored in IPFS a transaction id is generated. The hash value will be generated using SHA-256. The hash and the transaction id obtained from the IPFS and the patient id will be appended. The appended transaction id, patient id and hash value of the file will be saved in the blockchain as a block. When the user requests for the file, the file will be fetched from the IPFS and hash value is generated. Then it will match the hash value from the IPFS and the stored hash value from the blockchain. If it matches then file will be decrypted and file can be viewed.

Step 1: Registration

- Hospital Registration: Hospital admin enters the hospital information into the portal and details are saved into the database. Server generates the unique hospital id.

- Doctor Registration: Hospital admin enters the doctor's details and server generates the doctor's id and link with the hospital. All this information is stored in the database.
- Lab Assistant Registration: Hospital admin enters the lab assistant's details and server generates the unique id and is linked with the hospital. All this information is stored in the database.
- Patient Registration: Hospital admin enters the patient's details and server generates the unique patient id and is linked with the hospital. All this information is stored in the database. Patient id is linked with the doctor's id under whom the patient is assigned.

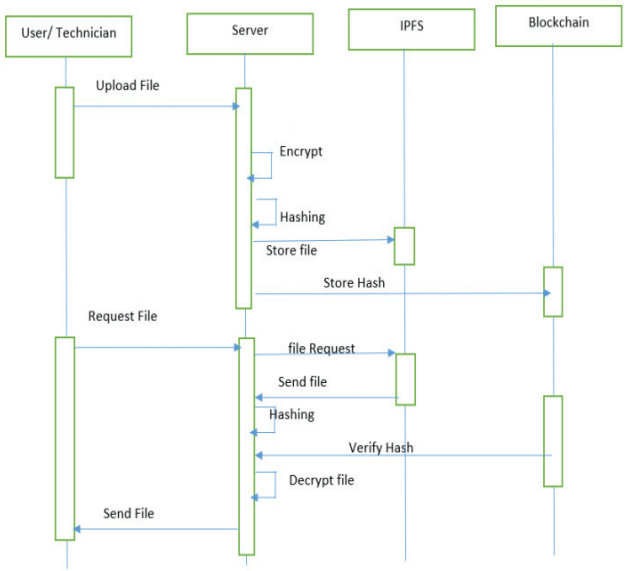

Fig. 3. Sequence Diagram

Step 2: Upload

Lab assistant or doctor can login into the portal and upload the patient's health status and other suggestion or information. Server generates the password to encrypt the file and send the email to the patient's email. Before encrypting the file server generates the hash value of the file using SHA-256 algorithm. For file encryption AES symmetric algorithm is used. The encrypted file is saved in the IPFS using API. Once the encrypted file is saved, IPFS returns the IPFS hash value to retrieve the file later. The file id, patient id, hash value of file, IPFS hash are stored in the Ethereum blockchain. No report information are stored in the server and stored in the distributed environment.

Step 3: Acess Report

When the patient wants to view or download his/her report, needs to send request to the Ethereum blockchain. The report information is retrieved from the blockchain and displayed. The file patient wants to view or download, is retrieved from the IPFS. The retrieved file will be in encrypted format. Patient has to enter the password to decrypt the file. Once the file is decrypted, the hash is generated and verify it with the value that is retrieved from the blockchain. If the lab assistant or doctor wants to view patient's record, he/she has to send request to the patient. Once the patient shares the key, the file can be decrypted and viewed.

IV. Implementation and Results

The implementation of distributed storage model uses IPFS distributed file system and blockchain. The uploaded file is stored in IPFS and hash of the transaction is stored in blockchain. The setup uses python anaconda, NetBeans IDE, Solidity IDE, MetaMask. The setup is performed on Intel Coe i5 processor,8250U CPU @ 1.60GHz running Window x64-based processor with 8GN and 1TB of local storage.

A. Flow chart for uploading file

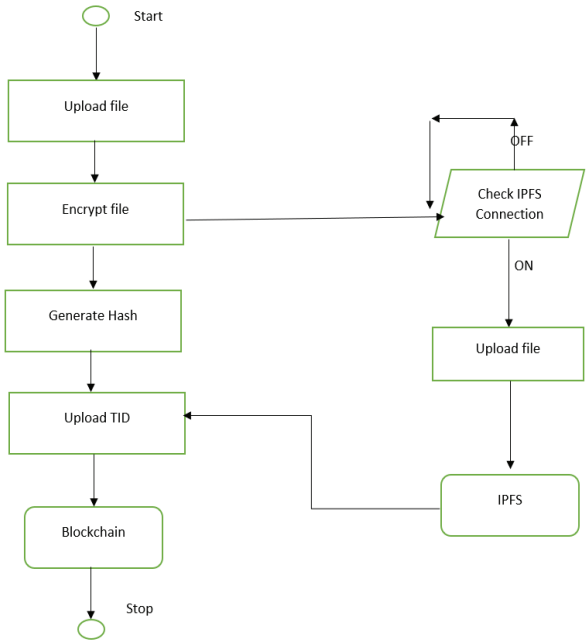

Fig. 4. Flow chart for uploading the file.

In the Fig.4, it is shown that the technician/doctor can upload the file. Before uploading the technician/doctor needs to ask permission from the patient to upload the file. Once the patient permits only then the file will be uploaded. The server encrypts the file using AES symmetric encryption using patient Id as the key for encryption. The server uploads the encrypted file to IPFS. Before uploading the file, the server checks for connection. Once the file is uploaded to the IPFS it returns the transaction id to the server. Then the server generates the hash of the encrypted file using SHA-256. Then patient id, hash value of the file and the transaction id is appended and stored in Blockchain.

B. Flowchart for downloading the file

In the Fig.5, it is shown that the user requests for the file to be downloaded/viewed to the server. The patient can login to view/download his/her file to the system. When the technician/doctor wants to view the file, they need to ask permission from the patient. Once the patient grants the permission the server will fetch the file from the IPFS. Before fetching it will check for the connection of IPFS. Simultaneously the Tid i.e, transaction id, patient id and the hash of the file is fetched from Blockchain. The server generates the hash value of the fetched file i.e. from IPFS by using SHA-256. Then it verifies it with the fetched hash value from Blockchain. If it is successful then the server will decrypt the file and can be accessed by the user.

C. Result Analysis

- Privacy and Security: The privacy of the user is handled in this system. The AES symmetric key encryption is used to provide the privacy of the user. When the lab assistant uploads the report the key of the report is sent to the respective patient through mail. The report can be decrypted only by using that key or else the report will not be decrypted. When the doctor wants to view or download the report, he/she needs to request the key from the patient. The patient will login to his/her system and send (mail) the key to the doctor. Even when the lab assistant has to upload the report, he/she has to request the permission from the patient for the upload. Once the patient grants the permission then the lab assistant can upload the report.

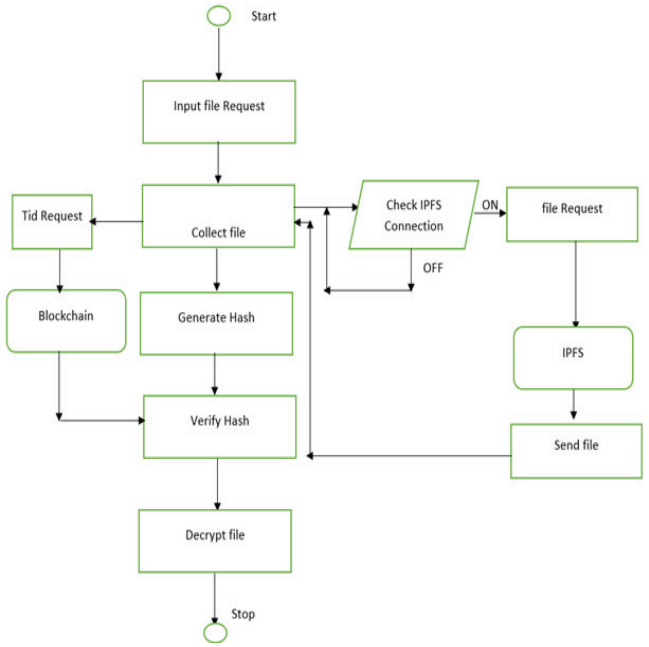

Fig. 5. Flow chart for downloading the file.

- Integrity and Immutability: Once the report is uploaded by the lab assistant then it cannot be reverted back or even edited. If there are changes in the report then a new copy of the report will be uploaded. And once the report is uploaded it cannot be deleted from the blockchain. It will always be stored in the blockchain.
- Transparency: If a patient wants to consult a new doctor, then at first the admin of the hospital needs to assign the new doctor to the patient only then the doctor can have access to the patient. Once the new doctor is assigned to the patient, he/she can view all the details of the patient. If the new doctor wants to view the report, then he/she should request the key from the patient. Once the patient sends the key the report can be viewed by the doctor. So, any doctor can view the report of patient only if the admin and the patient allow access to the doctor.
- Validation of data: While uploading the report the hash value of the file is calculated by using SHA-256 hash function then the file is uploaded to IPFS and the hash value of the file is stored in blockchain. When the user requests the file, it is retrieved from the IPFS and hash value of the file is calculated. Then it is compared with hash value that is stored in blockchain. If there is change in the file then the compare operation will fail. Thus, the data is validated.
- Storage: The file is stored in IPFS and the metadata of the file is stored in blockchain rather than storing the entire file in blockchain. The IPFS is a distributed peer-to-peer system where it stores the file as chunks of file in distributed nodes. Thus, there is not error when downloading the file even if some nodes are not available.

```
>>select * from patient_registration where hid='5'
Id for hospital--4
??????????????????????????????????C:/Users/hp/Documents/NetBeansProjects/Ipfs/web/
hid==========5
10-03-2021
11-39-26
report>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>C:/Users/hp/Documents/NetBeansProjects/Ipfs/web/persmission.pdf
5_4_10-03-2021_11-39-26.pdf
>>>b4daa6d2e3a94cfdc74f583fd5b624a8d0aa8731ededa2aca1757b9d9714bc3e
Sucess
```

Fig. 6. Ipfs_add

The doctor/lab assistant will upload the patients report to the server. Prior to the upload they need to seek permission from the patient. Once the patient approves the report is uploaded to the IPFS. When the file is uploaded, the filename is changed to custom file name which contains the hospital id, patient id, date and time. Simultaneously hash function (SHA-256) is applied to the file by the server.

```
5_4_10-03-2021_11-39-26_enc.pdf
File exist
<ipfshttpclient.client.base.ResponseBase: {'Name': '5_4_10-03-2021_11-39-26_enc.pdf',
                'Size': '176686'}>
5_4_10-03-2021_11-39-26_enc.pdf
QmQmi9eU5GfyM2UTn9kTwYXHDUZqkmLmG2xhyedTzGDDHc
176686
old data ##5_3_10-03-2021_11-36-02_enc.pdf@@QmbnVPw2xfRQJp92NviUNHF4bCqDu2pm97BddQqAmhc3Zs
resp= b'\xe91M\xba\xc9%wm@\xd8\x9aJ\x07;X\xf32\x004\xfe\xbc\x82\x99\x7f\xe7\x19\x04~\x07/\x9c6'
```

Fig. 7. Access the stored file in Blockchain.

In the Fig.7, it is shown the file that are uploaded in the blockchain contains filename, hash value of the file and transaction id of IPFS. The filename contains the hospital id, patient id, date and time when the file is uploaded. The old data shows the previous file stored in the blockchain. In the Fig.8 it is shown the data that is stored in a block of blockchain. Each block consists of name of the file, hash value of the file, ipfs_hash value and size of the file.

Fig. 8. Screenshot of Remix IDE after uploading the File

V. Conclusion

In this paper, distributed storage model using IPFS and blockchain is proposed to solve the existing problem of storage and access of block from blockchain. In the proposed model, we are storing the encrypted file in IPFS and the transaction id of the IPFS in the blockchain rather than storing the entire file in the blockchain. And in the blockchain the filename, hash value of the encrypted file and the transaction id fetched from IPFS is stored thus reducing the size of the block. So, when the file is requested to be viewed the encrypted file is downloaded from IPFS is verified it with file from blockchain. Thus, achieving the integrity and efficiently of the file. The patients can provide access to other users to view/download his/her report, and even have control over his/her data, hence improving data security.

References

[1] Rahalkar, Chaitanya, and Dhaval Gujar. "Content Addressed P2P File System for the Web with Blockchain-Based Meta-Data Integrity." In 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1-4. IEEE, 2019.

[2] Nyaletey, Emmanuel, Reza M. Parizi, Qi Zhang, and Kim-Kwang Raymond Choo. "BlockIPFSblockchain-enabled interplanetary file system for forensic and trusted data traceability." In 2019 IEEE International Conference on Blockchain (Blockchain), pp. 18-25. IEEE, 2019..

[3] Chen, Yongle, Hui Li, Kejiao Li, and Jiyang Zhang. "An improved P2P file system scheme based on IPFS and Blockchain." In 2017 IEEE International Conference on Big Data (Big Data), pp. 2652-2657. IEEE, 2017.

[4] Kumar, Randhir, and Rakesh Tripathi. "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain." In 2019 Fifth International Conference on Image Information Processing (ICIIP), pp. 246-251. IEEE, 2019.

[5] Kumar, Randhir, Ningrinla Marchang, and Rakesh 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), pp. 1-5. IEEE, 2020.

[6] Huang, Huawei, Jianru Lin, Baichuan Zheng, Zibin Zheng, and Jing Bian. "When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues." IEEE Access 8 (2020):

[7] Nizamuddin, Nishara, Haya R. Hasan, and Khaled Salah. "IPFS-blockchain-based authenticity of online publications." In International Conference on Blockchain, pp. 199-212. Springer, Cham, 2018.

[8] Nizamuddin, Nishara, Khaled Salah, M. Ajmal Azad, Junaid Arshad, and M. H. Rehman. "Decentralized document version control using Ethereum blockchain and IPFS." Computers & Electrical Engineering 76(2019):183-197.

[9] Xu, Quanqing, Zhiwen Song, Rick Siow Mong Goh, and Yongjun Li. "Building an ethereum and ipfs-based decentralized social network system." In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pp. 1-6. IEEE, 2018.

[10] Yadav, Nikhil, and V. Sarasvathi. "Venturing Crowdfunding using Smart Contracts in Blockchain." In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 192-197. IEEE, 2020.

[11] Nithin, M., S. Shraddha, Nishita Vaddem, and V. Sarasvathi. "HyperIoT: Securing Transactions in IoT through Private Permissioned Blockchain." In 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1-6. IEEE, 2020.

[12] Gururaj, H. L., A. Manoj Athreya, Ashwin A. Kumar, Abhishek M. Holla, S. M. Nagarajath, and V. Ravi Kumar. "BLOCKCHAIN: A NEW ERA OF TECHNOLOGY." Cryptocurrencies and Blockchain Technology Applications (2020): 1-24.

[13] Venkatesan, Subramanian, Shubham Sahai, Sandeep Kumar Shukla, and Jaya Singh. "Secure and Decentralized Management of Health Records." In Applications of Blockchain in Healthcare, pp. 115-139. Springer, Singapore, 2021.

[14] Gururaj, H. L., Athreya A. Manoj, Ashwin A. Kumar, S. M. Nagarajath, and V. Ravi Kumar. "Adoption of pets in distributed network using blockchain technology." International Journal of Blockchains and Cryptocurrencies 1, no. 2 (2020): 107-120.

[15] Charles, Wendy Marie. "Accelerating Life Sciences Research with Blockchain." In Applications of Blockchain in Healthcare, pp. 221-252. Springer, Singapore, 2021.

[16] Kumari, Meet, Meenu Gupta, and Chetanya Ved. "Blockchain in Pharmaceutical Sector." In Applications of Blockchain in Healthcare, pp. 199-220. Springer, Singapore, 2021.