Secure DocVault Using Blockchain & IPFS

Smt. Rubina
Senior Grade Lecturer
Department of Computer Science & Engg,
Government Polytechnic, Bagalkot, Karnataka

Smt. Sujatha P
Senior Grade Lecturer
Department of Computer Science & Engg
Government Polytechnic, Bagalkot, Karnataka

Smt Malati B Sajjan
Lecturer
Department of Computer Science & Engg
Government Polytechnic, Vijayapur, Karnataka

---

1. Abstract

In the past few years, the Blockchain technology has gained tremendous amount of trust for its security because of its decentralized in nature. Data plays very important role. Data from government or non-government document plays very important role in day-to-day life. The interference in the data change is irrelevant which causes the data to lose and data stolen which led to bigger problems. To overcome this issue, this proposed work is implemented. This work uses encryption methods to secure the data. The data could be any document e.g. Driving license, lease documents etc. The data stored on the website cannot be accessed by any other party apart from the user itself. To achieve this type of security the technologies used are Blockchain and IPFS.

Keywords : Blockchain; Encryption; InterPlanetary File System (IPFS)

2. Introduction

Decentralized technologies have ushered in a new era of data storage and interaction, offering novel solutions to traditional centralized systems. Among these technologies, blockchain stands out as a distributed and immutable ledger, while the InterPlanetary File System (IPFS) provides a decentralized and peer-to-peer file storage network. The integration of IPFS with blockchain platforms like Ethereum presents a compelling opportunity to create a robust decentralized file storage and interaction system that combines the strengths of both technologies.

Conventional centralized file storage systems suffer from single points of failure, limited scalability, and potential security vulnerabilities. Furthermore, reliance on intermediaries for file interaction introduces risks and compromises user control over data. To overcome these challenges, exploring decentralized approaches that leverage blockchain technology and

distributed file storage systems like IPFS is imperative.

3. Literature Survey

Decentralized storage systems have gained significant attention in recent years due to their potential to address the limitations of traditional centralized storage solutions. Researchers and industry experts have explored various approaches to achieve decentralized and secure storage, with the integration of blockchain-based file storage and InterPlanetary File System (IPFS) emerging as a promising solution.

Li et al. (2017) proposed a decentralized storage framework using blockchain technology, highlighting its ability to provide tamper-resistant and distributed data storage. The study emphasized the immutability and transparency offered by blockchain, enabling secure and auditable storage of sensitive information. Similarly, Smith et al. (2018) conducted a comparative analysis of decentralized storage systems, emphasizing their fault tolerance, scalability, and resistance to censorship.

The integration of IPFS with blockchain technology has been a subject of extensive research. Juan et al. (2016) introduced the concept of IPFS, a peer-to-peer distributed file system that aims to create a permanent and decentralized web. Their study demonstrated how IPFS addresses some of the limitations of traditional HTTP-based systems, such as content addressing and data deduplication. Building on this work, Nakamoto (2008) introduced blockchain technology with the creation of Bitcoin, a decentralized cryptocurrency. Subsequent research explored the potential applications of blockchain beyond cryptocurrencies, including its use in decentralized storage.

Smart contracts, a feature of blockchain platforms like Ethereum, have been leveraged in decentralized storage systems. Xu et al. (2019) proposed a smart contract-based approach for decentralized file storage, ensuring data integrity and availability. The study emphasized the use of Ethereum's blockchain to establish trust and automate storage-related operations, enhancing the security and reliability of the system.

Researchers have also investigated the practical implementation and performance of decentralized storage systems. Santos et al. (2020) conducted a performance evaluation of IPFS for file storage, analyzing factors such as latency, throughput, and resource consumption. Their findings demonstrated the feasibility of using IPFS for decentralized storage, although challenges related to scalability and data redundancy were highlighted.

These approaches offer benefits such as immutability, fault tolerance, and transparency, addressing concerns related to data security and privacy. The integration of smart contracts further enhances the capabilities of decentralized storage systems. However, challenges such as scalability and resource consumption need to be addressed for wider adoption in real-world applications

4. Proposed Methodology

In this work, we used the two technologies.

1. Ethereum Blockchain which is used to store the data about user file as the hash file.
2. IPFS (Inter Planetary File System) it is used for the sharing data in a distributed file system.

Alorithm for Secure Document Vault

Step 1: - Get the data or file from the user and store in the object variable.

Step 2: - Convert the file into file Buffer.

Step 3: - Send the file document to the IPFS.

Step 4: - Then IPFS create a node for the file revert the hash of the node where the file is store.

Step 5: - Check whether the data existed in the block chain if existed print the data is already available.

Step 6: - Ff not store the hash into the block chain with some additional data like (document name, categories, existence etc)

Step 7: - Display the file from the block chain.

- **Getting a data file from the user**

To get the user data we must call the document object function which helps to fetch the data file from the user's system and store it in the object variable. For this, we used to react for the user experience where the react will handle the getting file function.

- **Convert the file into file Buffer.**

We will convert the file into the file buffer which acts as the temporary file object. without affecting the original file once it saved it will automatically update the file this will allow the user to elaborate its documents before updating.

- **Send the documents to the IPFS.**

First we must send the document to the IPFS node. Where the IPFS will evaluate and then check whether there is a duplicate or not and store the file in the node and send back the IPFS hash. The hash is working in the principle of DAGs (directed acyclic graphs) specifically, they use Merkle DAGs this will help uniquely identifier that is a hash of the node's contents.

In this proposed paper we are using the 'infra' which is the public IPFS API for storing the document. After receiving the hash code from the IPFS we will store the data in the blockchain. The main drawback is , by using the hash code anyone can access the file which is not efficient , so to overcome this we encrypt furthermore for privacy.

- **Checking for duplicate**

Checking for the duplicate is important if the same document object is available at the blockchain will lead to wastage of the blockchain as well as data redundant. Which lead to further complication in the blockchain.

- **Store in the blockchain**

After getting the IPFS hash. We further encrypt the data from the IPFS by using the RSA Encryption algorithm with user details and categories to which that document

belongs and store into the blockchain. After it will ask the gas to pay for a transaction to be completed.

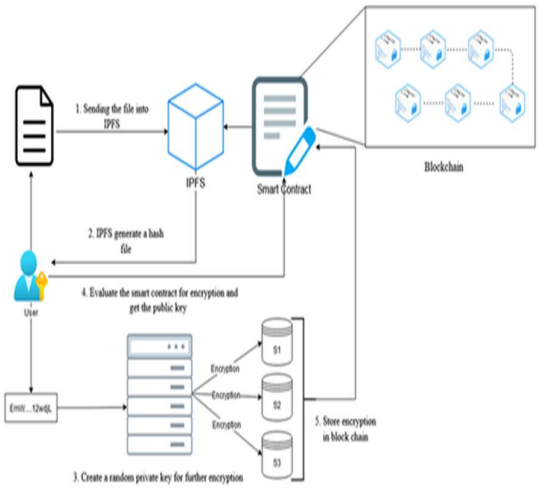


Fig 1.1 Working Techology of the secure document vault.

Let us say the file random.jpg file will store in the block chain first it will send the doc to IPFS then IPFS will going to process it and send the hash code of the file back to program. Where the program will encrypt the hash and add random private key which look like.

"0xF42ba36FdaFe215c574D1f6a18A61d41 9044A915" +private Key only the user who has the same key can only access. If other than user who has a key, try to access it will be going to show the error and it will not show anything. After words it will store back into the block chain with some additional information like user id categories from which it is belongs and some more information like (Document name, categories, existence etc).

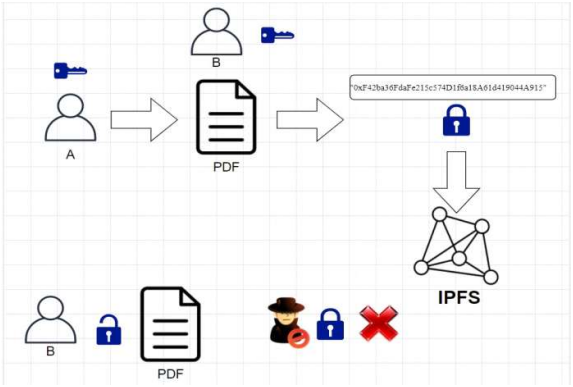


Fig 1.2: Key authentication

5. Results

Fig 5. 1 Category Page

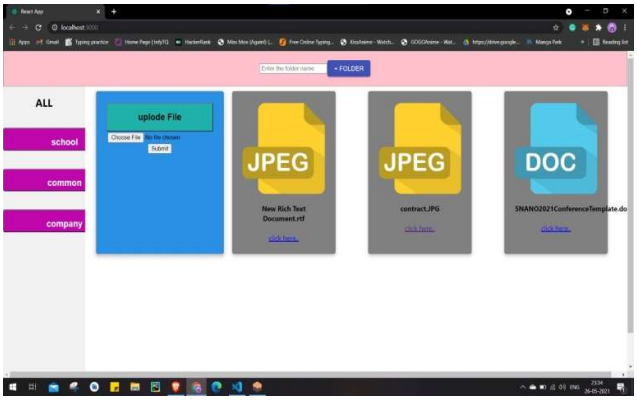


Fig 5. 2 Main Page

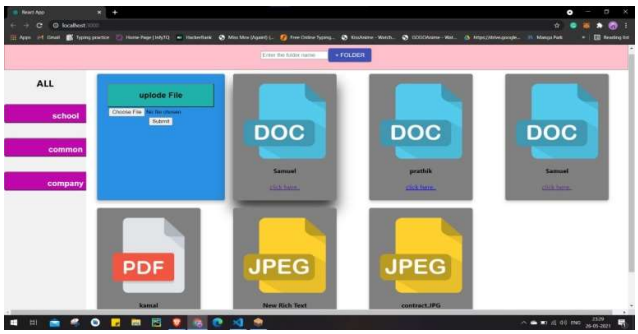


Fig 5.3 Console Page

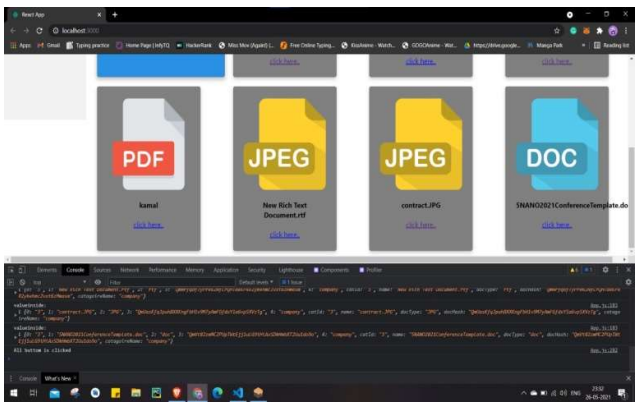
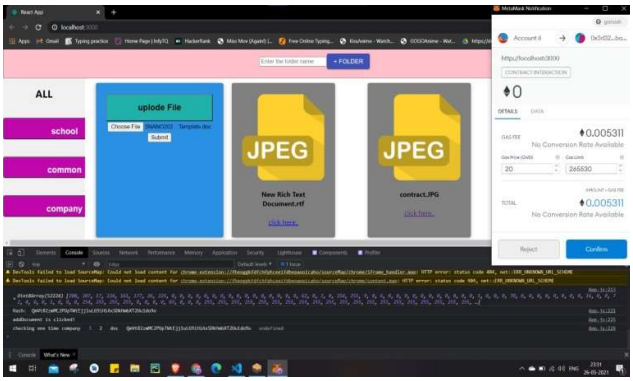


Fig 5.4 **Transaction Page**



6. Applications

1. Banking sectors they can use to store the private documents like bonds, investment documents.
2. In insurance company they can you it for validation of the documents of the users.
3. The users can store his personal or impotent documents.
4. The Inter-Planetary Version Control system (IPVC) is a distributed version control system similar to git but built on IPFS.

7. Conclusion

Secure Document Vault will help the user to store their personal and non-personal related documents which could be private. Our application provides the platform where the user can store their document. If they need, we provide the categories vies document to store which is helpful for the end user to find his/her document whenever he/she needs. The main purpose of our work is to provide the user to store their private file which are important to him either related to work, bank, bonds etc. and the interface where the user will be going to be used supposed to be the user-friendly.

8. References

[1]. Paras Pant; Ruchika Bathla; Sunil Kumar Khatri, “A Model to Implement and Secure Online Documentation using Blockchain”, 2019 4th International Conference on Information Systems and Computer Networks (ISCON).

[2] . MD. Soharab Hossain Sohan; Minhaz Mahmud; M A Baten Sikder; Fakir Sharif Hossain; Md. Rakibul Hasan, “Increasing Throughput and Reducing Storage Bloating Problem Using IPFS and Dual-Blockchain Method”, 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST).

[3] .Songyue Liu; Shangyang He, “Application of Block Chaining Technology in Finance and Accounting Field”.

[4]. Jammulapati Ravi Teja, “Proposing method for Public record maintenance using Block chain”.

[5] .Qiuhong Zheng; Yi Li; Ping Chen; Xinghua Dong, “An Innovative IPFS-Based Storage Model for Blockchain”

[6]. Yongle Chen; Hui Li; Kejiao Li; Jiyang Zhang, “An improved P2P file system scheme based on IPFS and Blockchain”

[7] .Shankar K; “An Optimal RSA Encryption Algorithm for Secret Images”

[8] .Deepak K. Tosh, Sachin Shetty, Xueping Liang, Charles Kamhoua, Laurent Njilla