History of Medicine, 2024, 10(2): 349-356

DOI: 10.17720/2409-5834.v10.2.2024.030

DECENTRALISED SECURE CLOUD STORAGE USING BLOCKCHAIN

Ramesh[1], Shivani[2], Venkata Naga Aditya Panuganti[2], Shiva Sai Thodeti[2] , Sameer MD[2]

[2]UG Scholar, [1,2]Department of Computer Science and Engineering

[1,2]Kommuri Pratap Reddy Institute of Technology, Ghatkesar, Hyderabad, Telangana.

ABSTRACT

Cloud storage is crucial for modern computing, offering convenient data access from anywhere with internet connectivity. Traditional cloud storage is centralized, posing risks of single points of failure, data breaches, and privacy concerns, as users must trust service providers for data protection. This has driven the demand for decentralized secure cloud storage. Blockchain-based storage solutions offer a promising approach, ensuring data integrity, privacy, and availability by distributing data across multiple nodes in a network. Leveraging blockchain's immutable ledger, the system verifies data authenticity and employs smart contracts for secure access and management. This research introduces a decentralized secure cloud storage system using blockchain, representing a significant shift in data storage and management. By distributing data across nodes, it eliminates risks associated with centralization. Smart contracts enforce access controls and encryption, enhancing security and privacy. Users gain greater ownership and control over their data through key access management, supporting data sovereignty by adhering to jurisdictional laws and regulations. This proposed system has the potential to revolutionize data storage practices, offering a secure and privacy-focused alternative to traditional centralized cloud services.

Keywords: Decentralized Storage, Blockchain, Data Integrity, Smart Contracts, Data Sovereignty, Cloud Security.

1. INTRODUCTION

Information has become the most important asset for anybody because to the expanding sectors of information technology, the Internet of Things, and the digitization of all businesses, organisational activity, and initiatives. The most powerful thing in the world today is data. Given the volume of data and its continual growth, it's crucial to arrange its storage to make it both secure and easily accessible. Databases are being employed as a data warehouse for this purpose.Due to the value of data and the lack of available storage, databases are replicated, distributed, and backed up in various methods. Data is stored by individuals in the cloud services offered by various private businesses. To store their data, organisations build up their data centres all over the world. Data is dispersed and replicated to various servers located in various locations for security and bandwidth reasons. This appears to offer a practical answer for the handling of data that is accumulating quickly.The rise in demand for storage, where the data can be easily accessible from anywhere and at any time, has led to the increasing popularity of Cloud Storage systems. The Cloud storage implementes a central repository. This storage is vulnerable to cyber-attacks, once an attacker gains access to the system complete confidential information is under breach. If a file gets modified there is no way of getting hands on the original data.

2. LITERATURE SURVEY

With the explosive growth of data, the security and efficiency of storage become especially important, and blockchain technology [1,2,3,4,5,] provides a new way of thinking for data storage methods.

Currently, research related to blockchain applications in storage is in the nascent stage [6], and decentralized storage research on the protection of storage resources usually stops at the level of "key encryption" protection, which leaves resources exposed to threats for a long time. For example, resources remain vulnerable if encryption keys are exposed or if malicious nodes do not remove their fragments in response to the owner’s request. Moreover, there is not much research on the availability of stored files to capture the probability of losing resources after they are uploaded to the network. With the exploration and practice of scholars [7], the application of blockchain technology to the field of data storage mainly includes two approaches: Data is written directly to the block, the block header contains the hash, random value, and data hash of the previous block, and the block body is loaded with the data to be saved. After the block is verified by consensus, it can be synchronized to all nodes on the chain, which ensures the data’s immutability, but this approach requires saving the same data on all nodes, which is more redundant and causes waste of storage resources if the data is too large, and also the data synchronization speed becomes slower. This approach is only applicable to scenarios where the amount of data is small and important, such as information traceability [8]. Data is not written directly to the block, but the file summary hash, file location, and other information are written to the block, the real data is stored in the file system, and the integrity of the file data can be verified through the calculation of the hash function. Combining the blockchain with the file storage system, the blockchain manages files through smart contracts to reach a series of operations about file uploading and downloading. This approach is universal, not bound to the size and importance of files, and can be applied to most scenarios about storage [9,10]. In terms of integrity verification of stored data, the literature [11] proposes a blockchain-based scheme for verifying data integrity by using the Merkle tree structure in the blockchain to store metadata of data, but no protection scheme is proposed for the privacy of file data. The main differences between the proposed method and the existing decentralized storage framework include: the traditional distributed storage system cannot solve the problem of mutual trust between joint nodes, whereas blockchain technology can solve this problem well and is the most successful decentralized system at present; compared with the existing blockchain-based distributed storage system, the proposed method does not directly store the file content but only saves the hash value of the corresponding file, and the specific file content can be retrieved in IPFS according to the hash value, which solves the problem that blockchain cannot save large files.

3. PROPOSED METHDOLOGY

Dataset Selection: The first step in our research involves the careful selection of a dataset. This dataset should be representative of the types of data commonly stored in cloud storage systems. It may include various file formats, sizes, and structures to ensure the robustness of our proposed solution.

Data Preprocessing: Once the dataset is chosen, data preprocessing is undertaken to clean and organize the data. This step involves handling missing values, standardizing formats, and addressing any outliers or anomalies in the dataset. Preprocessing ensures that the subsequent analysis is based on high-quality, reliable data.

Data Splitting: To evaluate the performance of our decentralized secure cloud storage system, we need to divide the dataset into training and testing sets. The training set is used to train our model, while the testing set serves as an independent dataset to assess the system's performance. This step is crucial for unbiased evaluation and to simulate real-world scenarios.

Performance Evaluation: With the dataset split, the next phase involves the actual implementation of our decentralized secure cloud storage system using blockchain technology. During this implementation, we carefully monitor and evaluate the system's performance. Metrics such as data retrieval speed, security measures, and overall system efficiency are assessed to ensure that the proposed solution meets the desired objectives.

Prediction from Test Data: After successful implementation and performance evaluation, the system is put to the test using the independent testing dataset. This step involves predicting outcomes based on the testing data and comparing these predictions with the actual results. The accuracy and reliability of the predictions serve as key indicators of the system's effectiveness in real-world scenarios.

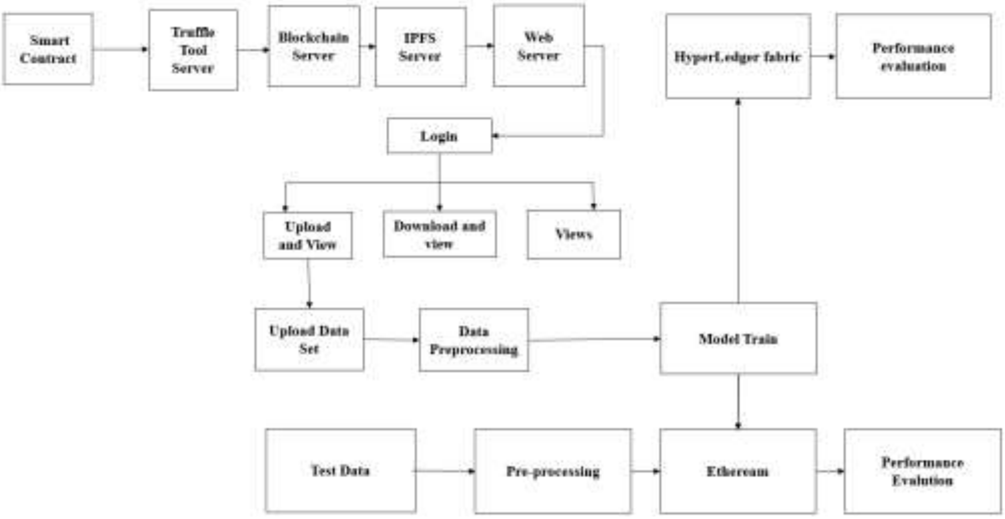


Figure 1: Block Diagram of Proposed System.

Ethereum

Ethereum is a decentralized blockchain platform that allows developers to build decentralized applications (Apps) and execute smart contracts. It was launched in 2015 by Vitalik Buterin and quickly became one of the most popular blockchain platforms in the world, second only to Bitcoin in terms of market capitalization.

Ethereum's main innovation is the ability to create smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. These smart contracts are executed on the Ethereum Virtual Machine (EVM), which is a decentralized, Turing-complete virtual machine that runs on the Ethereum network.

The Ethereum network also has its own cryptocurrency called Ether (ETH), which is used to pay for transaction fees and computational services on the network. ETH is also used as a store of value and traded on cryptocurrency exchanges.

Advantages of Ethereum

Ethereum provides several advantages over other blockchain platforms and traditional systems. Here are some of the main advantages of Ethereum:

Smart Contracts: Ethereum's main innovation is the ability to create smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This allows for secure and automated execution of complex agreements without the need for intermediaries or third parties.

Decentralization: Ethereum is a decentralized platform, which means that it is not controlled by any single entity or organization. This provides a level of trust and transparency, as there is no single point of failure or vulnerability.

Interoperability: Ethereum's blockchain is open-source and allows for interoperability with other blockchain platforms, making it easier to integrate with existing systems and applications.

Programmable: Ethereum's blockchain is programmable, which means that developers can create custom applications and smart contracts that meet their specific needs. This allows for more flexibility and customization than traditional systems.

Security: Ethereum's blockchain is secured through cryptographic algorithms and consensus mechanisms, making it resistant to hacking and fraud. Additionally, smart contracts on the platform are auditable and transparent, which helps to reduce the risk of fraud and corruption.

Tokenization: Ethereum enables the creation and exchange of tokens, which can represent assets, securities, or other digital assets. This makes it possible to create new business models and revenue streams that were previously not possible.

Blockchain

Blockchain is a decentralized, digital ledger technology that is used to record and store data in a secure and transparent manner. It is a distributed ledger, meaning that it is maintained by a network of computers, rather than being controlled by a single entity. Each block in the chain contains a set of transactions, and once a block is added to the chain, it cannot be altered or deleted. This makes blockchain an immutable and tamper-resistant technology that is particularly well-suited for storing and transmitting sensitive data.

Blockchain technology is perhaps best known for its use in cryptocurrencies like Bitcoin and Ethereum, but it has a wide range of other potential applications as well. These include supply chain management, identity verification, voting systems, and more. The decentralized nature of blockchain means that it has the potential to disrupt a variety of industries and business models by enabling trust and transparency in transactions and data exchange.

Concepts

There are several key concepts that are important to understand when it comes to blockchain technology:

Decentralization: Blockchain is a decentralized technology, meaning that it is not controlled by any single entity, but rather maintained by a network of participants. This increases transparency, security, and resilience.

Distributed ledger: Blockchain technology uses a distributed ledger to record and store data. Each block in the chain contains a set of transactions, and once a block is added to the chain, it cannot be altered or deleted.

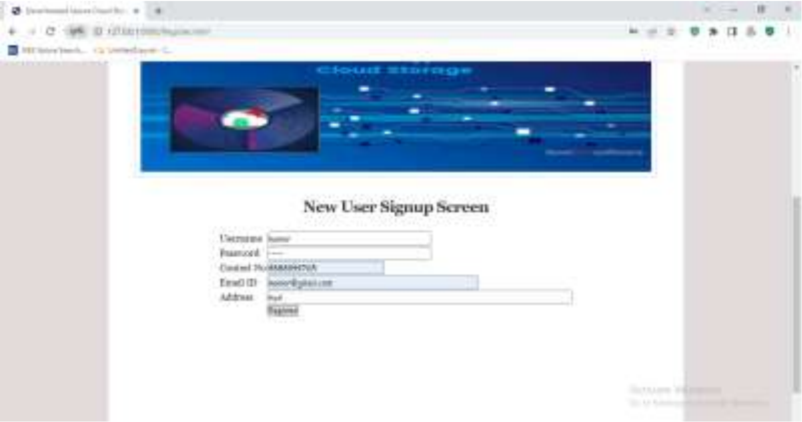
Cryptography: Blockchain technology uses advanced cryptographic algorithms to secure transactions and data exchange, making it highly resistant to hacking and cyber-attacks.

Consensus mechanism: In a blockchain network, participants must agree on the validity of transactions before they are recorded on the blockchain. Different blockchain networks use different consensus mechanisms to achieve this, such as Proof of Work or Proof of Stake.

Smart contracts: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They can be used to automate complex transactions and ensure that all parties involved in a transaction adhere to the terms of the contract.

Tokenization: Blockchain technology enables the creation of digital tokens that can be used to represent a variety of assets, such as currencies, commodities, or even real estate.

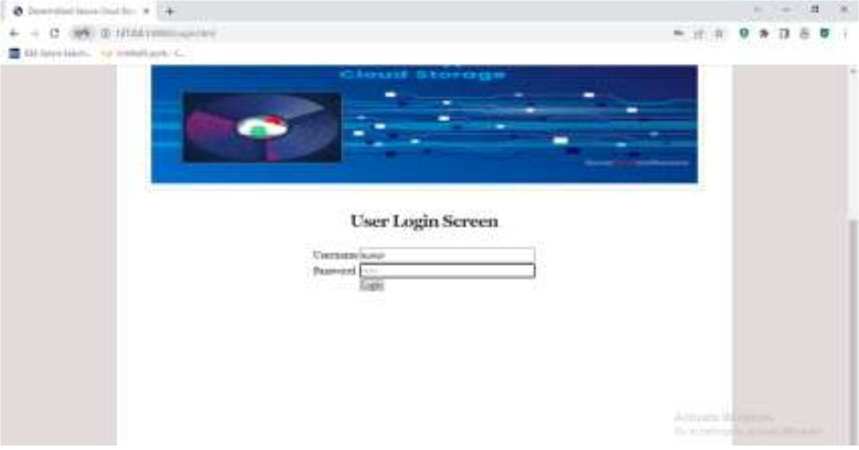
4. RESULTS AND DISCUSSION



New User Signup Screen

Username kumar
Password ••••••
Contact No 8888899765
Email ID kumar@gmail.com
Address Hyd
Register

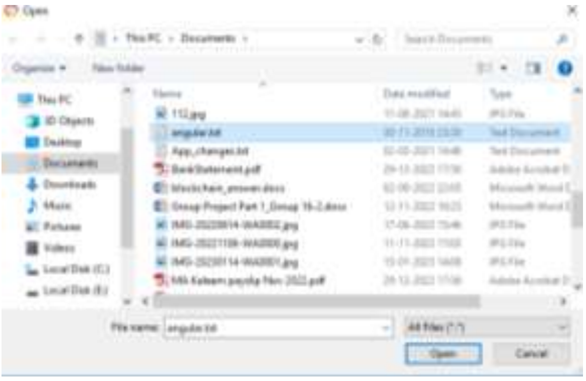
In above figure user is entering signup details and then press button to save client user data in Blockchain and get below output



User Login Screen

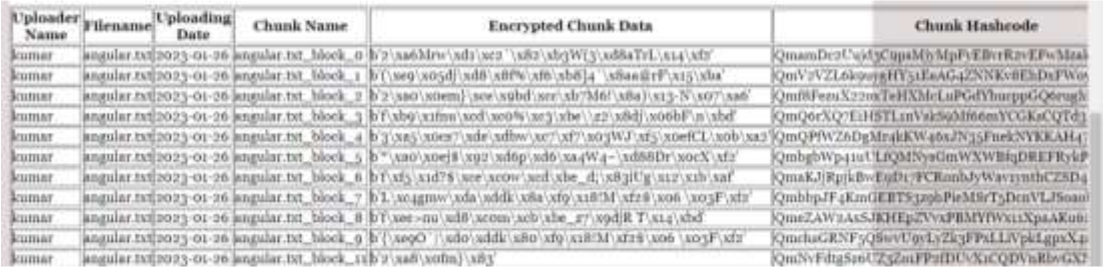
Username kumar
Password •••••
Login

In above figure user is login and after login will get below page



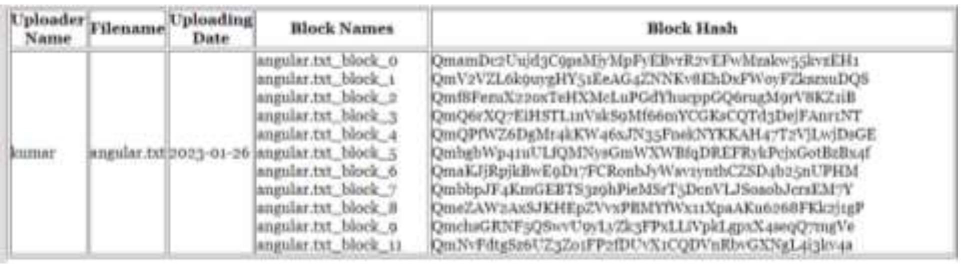
File name: angular.txt
All Files (*.*)

In above figure selecting and uploading file and then click on 'Open' and 'Submit' button to divide file into blocks and then encrypt each block and then save at different IPFS nodes and Blockchain and get below output



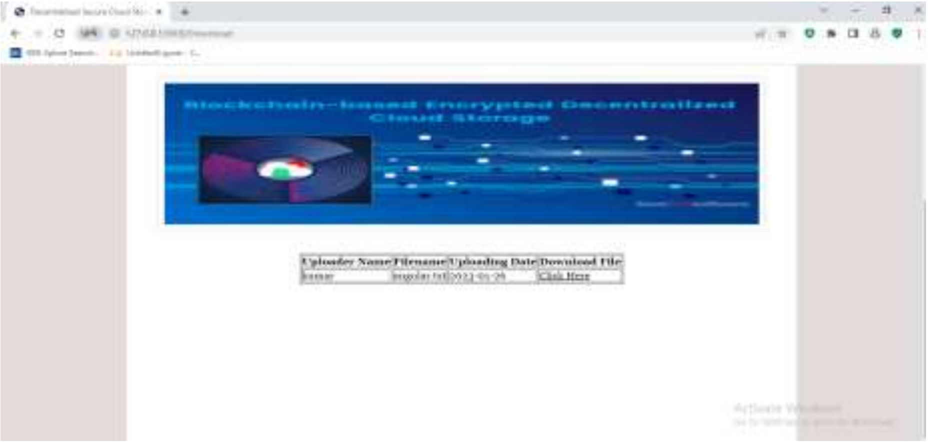
Uploader Name	Filename	Uploading Date	Chunk Name	Encrypted Chunk Data	Chunk Hashcode
kumar	angular.txt	2023-01-26	angular.txt_block_0	b'2\xa6Mrw\xd1\xe2`\x82\xb3W{3\xd84TrL\x14\xf2'	QmamDc2Uujd3C9paMiyMpFyEBvrR2vEFwMzak
kumar	angular.txt	2023-01-26	angular.txt_block_1	b'(\xe9\x05dJ\xd8\x8f%\xf6\xb8]4`\xf8aa@rF\x15\xba'	QmV2VZL6k9uygHY51EeAG4ZNNKv8EhDxFWoy
kumar	angular.txt	2023-01-26	angular.txt_block_2	b'2\xa0\x0em}\xce\x9bd\xcc\xb7M6!\x8a)\x13-N\x07\xa6'	Qmf8FezuX22oxTeHXMcLuPGdYhucppGQ6rugM
kumar	angular.txt	2023-01-26	angular.txt_block_3	b'f\xb9\x1fmn\xcd\xe0%\xe3\xbe\\z2\x8dj\x06bF\n\xbd'	QmQ6rXQ7EiHSTL1nVskS9Mf66mYCGKsCQTd3
kumar	angular.txt	2023-01-26	angular.txt_block_4	b'3\x85\x0ee7\xde\xdbw\xc7\xf7\x03WJ\xf5\x0efCL\x0b\xa2'	QmQPfWZ6DgMr4kKW46xJN35FnekNYKKAH47
kumar	angular.txt	2023-01-26	angular.txt_block_5	b'"\xa0\x0ej8\x92\xd6p\xd6\xa4W4~\xd88Dr\x0cX\xf2'	QmbgbWp41uULfQMNysGmWXWBfqDREFRykP
kumar	angular.txt	2023-01-26	angular.txt_block_6	b'f\xf5\x1d?8\xce\xc0w\xed\xbe_d;\x83iUg\x12\x1b\xaf'	QmaKJjRpjkBwE9D17FCRonbJyWav1ynthCZSD4
kumar	angular.txt	2023-01-26	angular.txt_block_7	b'1\x04gmw\xda\xddk\x8a\xf9\x18!M\xf28\x06`\x03F\xf2'	QmbbpJF4KmGEBTS329hPieMSrT5DcnVLJSoaob
kumar	angular.txt	2023-01-26	angular.txt_block_8	b'f\xee>nu\xd8\xc0m\xcb\xbe_z7\x9d|R T\x14\xbd'	QmeZAW2AxSJKHEpZVvxPBMYfWx11XpaAKu6
kumar	angular.txt	2023-01-26	angular.txt_block_9	b'{\xe9O`|\xd0\xddk\x80\xf9\x18!M\xf28\x06`\x03F\xf2'	QmchsGRNF5QSwvU9y1LyZk3FPxLLiVpkLgpxX4
kumar	angular.txt	2023-01-26	angular.txt_block_11	b'2\xa8\x0fm}\x83'	QmNvFdtgSz6UZ3Zo1FP2fDUvX1CQDVnRbvGXN

In above figure same file is divided into 11 blocks and we can see name of uploader, filename, chunk (block name), encrypted data and its hash code address of file stored in IPFS and Blockchain. Similarly you can upload other files and while uploading you need to upload small files as big files will take lots of time for encryption. Now click on 'View Blocks' link to get below page



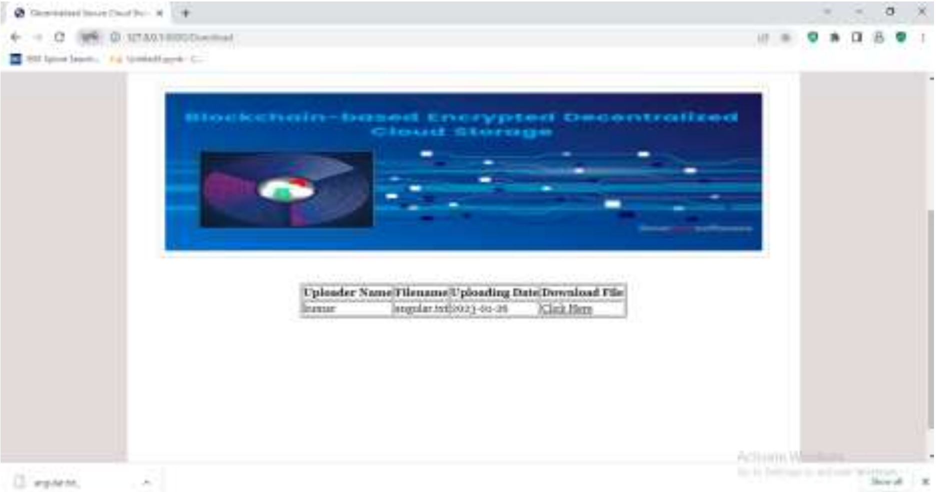
Uploader Name	Filename	Uploading Date	Block Names	Block Hash
kumar	angular.txt	2023-01-26	angular.txt_block_0 angular.txt_block_1 angular.txt_block_2 angular.txt_block_3 angular.txt_block_4 angular.txt_block_5 angular.txt_block_6 angular.txt_block_7 angular.txt_block_8 angular.txt_block_9 angular.txt_block_11	QmamDc2Uujd3C9paMiyMpFyEBvrR2vEFwMzakw55kvzEH1 QmV2VZL6k9uygHY51EeAG4ZNNKv8EhDxFWoyFZksrxuDQS Qmf8FezuX22oxTeHXMcLuPGdYhucppGQ6rugM9rV8KZ1iB QmQ6rXQ7EiHSTL1nVskS9Mf66mYCGKsCQTd3DeJFAnr1NT QmQPfWZ6DgMr4kKW46xJN35FnekNYKKAH47T2VJLwjDsGE QmbgbWp41uULfQMNysGmWXWBfqDREFRykPcjxGotBzBx4f QmaKJjRpjkBwE9D17FCRonbJyWav1ynthCZSD4b25nUPHM QmbbpJF4KmGEBTS329hPieMSrT5DcnVLJSoaobJcraEM7Y QmeZAW2AxSJKHEpZVvxPBMYfWx11XpaAKu6268FKk2j1gP QmchsGRNF5QSwvU9y1LyZk3FPxLLiVpkLgpxX4seqQ7mgVe QmNvFdtgSz6UZ3Zo1FP2fDUvX1CQDVnRbvGXNgL4i3kv4a

In above figure for each file user can see name of file and its block name and stored address of those blocks in hash code format. Now click on 'Download File' link to get below figure



Uploader Name	Filename	Uploading Date	Download File
kumar	angular.txt	2023-01-26	Click Here

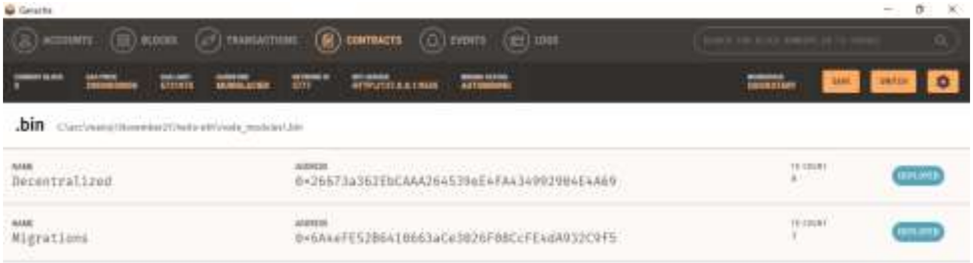
In above figure user can see list of uploaded files and then click on 'Click Here' link to download the file



Uploader Name	Filename	Uploading Date	Download File
kumar	angular.txt	2023-01-26	Click Here

In above figure in browser status bar we can see file is downloading and similarly you can upload and download any type of file. After downloading you can see file in encrypted format.

In Ganache also we can see Decentralized Smart Contract deployed like below figure



NAME	ADDRESS	TX COUNT	
Decentralized	0×26673a362EbCAAA264539eE4FA4349029B4E4A69	8	DEPLOYED
Migrations	0×6A4eFE52B6418663aCe3826F08CcFE4dA932C9F5	1	DEPLOYED

5. CONCLUSION

The research presented explores the development of a decentralized secure cloud storage system utilizing blockchain technology. This innovative approach addresses the inherent vulnerabilities of traditional centralized cloud storage systems, such as single points of failure, data breaches, and privacy concerns. By leveraging blockchain's decentralized and immutable ledger, the proposed system ensures data integrity, privacy, and availability through distributed data storage across multiple nodes.

REFERENCES

[1] Qu, Y.; Pokhrel, S.R.; Garg, S.; Gao, L.; Xiang, Y. A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks. IEEE Trans. Ind. Inform. **2020**, 17, 2964–2973.

[2]nXu, C.; Qu, Y.; Luan, T.H.; Eklund, P.W.; Xiang, Y.; Gao, L. A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things. IEEE Internet Things J. **2022**, 9, 4371–4384.

[3] dos Santos Abreu, A.W.; Coutinho, E.F.; Bezerra, C.I.M. Performance Evaluation of Data Transactions in Blockchain. IEEE Lat. Am. Trans. **2021**, 20, 409–416.

[5] Kanade, V.A. A Blockchain-Based Distributed Storage Network to Manage GrowingData Storage Needs. In Proceedings of the 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India, 13–14 May 2021; pp. 365–368.

[6] Li, L.; Liu, Y.; You, I.; Song, F. A Smart Retransmission Mechanism for Ultra-Reliable Applications in Industrial Wireless Networks. IEEE Trans. Ind. Inform. **2022**, 1–9.

[7] Ullah, Z.; Raza, B.; Shah, H.; Khan, S.; Waheed, A. Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment. IEEE Access **2022**, 10, 36978–36994.

[8] Yin, H.; Zhang, Z.; He, J.; Ma, L.; Zhu, L.; Li, M.; Khoussainov, B. Proof of Continuous Work for Reliable Data Storage Over Permissionless Blockchain. IEEE Internet Things J. **2022**, 9, 7866–7875.

[9] Mughal, M.H.; Shaikh, Z.A.; Ali, K.; Ali, S.; Hassan, S. IPFS and Blockchain Based Reliability and Availability Improvement for Integrated Rivers' Streamflow Data. IEEE Access **2022**, 10, 61101–61123.

[10] Hasan, H.R.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Pesic, S.; Omar, M. Trustworthy IoT Data Streaming Using Blockchain and IPFS. IEEE Access **2022**, 10, 17707–17721.

[11] Wiraatmaja, C.; Zhang, Y.; Sasabe, M.; Kasahara, S. Cost-Efficient Blockchain-Based Access Control for the Internet of Things. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6.

[12] Sijie Chen, H.M.; Ping, J.; Yan, Z.; Shen, Z.; Liu, X.; Zhang, N.; Xia, Q.; Kang, C. A blockchain consensus mechanism that uses Proof of Solution to optimize energy dispatch and trading. Nat. Energy **2022**, 7, 495