IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

A Secure Decentralized Data Storage Framework Using Blockchain Technology

Ganesh J[1], Priyadharshini R[2], Swetha K[2] and Vaishnavi G[2]
Assistant Professor, Department of Computer Science and Engineering[1]
Student, Department of Computer Science and Engineering[2]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India
jaygan85@gmail.com[1] and swethakarthi05@gmail.com[2]

Abstract: *Cloud storage is one of the leading options to store massive data, however, the centralized storage approach of cloud computing is not secure. On the other hand, Blockchain is a decentralized data storage system that ensures data security. Any computing node connected to the internet can join and form peers network thereby maximizing resource utilization. Blockchain is a distributed peer to peer system where each node in the network stores a copy of blockchain thus making it immutable. In the proposed system, the user's file is encrypted and stored across multiple peers in the network using the IPFS (InterPlanetary File System) protocol. IPFS creates hash value. The hash value indicates the path of the file and is stored in the blockchain. This paper focuses on decentralized secure data storage, high availability of data, and efficient utilization of storage resources. Here is our take on using Block Chain technology as a decentralized data storage system. Wherein we use resiliency attacks to display the benefits of Block chain based decentralized data storage by performing key operations on our proposed decentralized structure.*

Keywords: Blockchain, Data Security, IPFS, Encryption, Smart Contract, Data Storage

I. INTRODUCTION

The proposed system revolves around Block chain technology, a decentralized implementation. Cloud storage is traditionally known for it's centralized system. Here, we are using Block Chain technology as a decentralized cloud storage system. To construct a model of decentralized data storage technology based on Block chain with the purpose to improve the security and confidentiality of information.

Blockchain - a distributed database, in which you can store any data or transactions. In blockchain stores information across a network of personal computers, and the result is not only decentralized, but the allocated space. Consequently, neither the company nor the people, nor any other trusted party is not the owner of the network. All people can use the system, and thus to maintain its operation, so one person is very difficult to crack or completely destroy the network [2].People are using their personal computers to store bundles of other user data, called blocks ("blocks") in the chronological chain ("chain"), hence the name "blockchain" literally "a chain of blocks." Blockchain-revolution can be divided into 3 categories: 1 Blockchain. 0 (cryptocurrency bitcoin), 2.0 (smart contracts) and 3.0 (the application). Bitcoin - is both a digital cash, currency and online payment system in which encryption methods provide control of aggregate monetary units and the confirmation of the transfer of funds, work without intermediaries and national central banks. Bitcoin was first established 9 years ago, January 9, 2008, to be precise an unknown person or group of people under the pseudonym Satoshi Nakamoto. Payments made in a decentralized virtual currency of any cryptocurrency like Bitcoin is written in such a public journal entries stored in the shared network on users' computers this cryptocurrency and continuously available for viewing. Thus, any transaction performed cryptocurrency impossible to alter or forge. Blockchain, At this point, if the user is interested in the "cloud" storage of files he has three options: download the data to your own server, to take advantage of centralized services such as Google Drive or Dropbox, a network for decentralized storage of files, like Freenet. Each of these options have their drawbacks; at first too high costs of customization and technical support, the second relies on an intermediary service owner, and often expensive, the third variant is characterized by a low rate service and is limited by the amount of storage space as well as the users of the service provided (or not at all) available memory for use at their discretion. Thanks to modern advanced information technology there is a fourth option, which will provide more space for storing data and high-quality service in a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

decentralized environment. This work is intended to prove the hypothesis that the option for data storage is the most secure. It is assumed that the data store based on technology blockchain invulnerable to attempts to disclosure of confidential information, as all data is protected using cryptographic techniques. Cryptographic encryption algorithms ensure high security of data against attempts of forgery or alteration of their content.

Another undoubted advantage of decentralized storage in terms of security is the fact that the data is spread to be divided into parts of the network and encrypted on the client side by cryptographic algorithms. Consequently, data all users are distributed across the network in an encrypted form in multiple copies in the safe from hacking free-space computer hard drives of people around the world. This paper includes a study of such a distributed data store, wherein the data storage is performed by entering into a contract between intelligent network nodes. Users in such a decentralized environment fall into two categories: host, renting storage space, and user-farmer, providing space of their own hard drive. For the provision of free farmer node receives the award from host-tenant as cryptocurrency.

II. MODELING AND ANALYSIS

Metamask

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications. MetaMask is developed by ConsenSys Software Inc., a blockchain software company focusing on Ethereum-based tools and infrastructure. MetaMask allows users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and securely connect to decentralized applications through a compatible web browser or the mobile app's built-in browser

Ethereum Network

It is an open-source, public blockchain based distributed computing platform. Ethereum uses smart contracts where one can add business logic to make decentralized applications as per the business requirements. Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority. Ether (ETH or Ξ) is the native cryptocurrency of the platform.

Peers

A blockchain network is comprised primarily of a set of peer nodes (or, simply, peers). Peers are a fundamental element of the network because they host ledgers and smart contracts. These are the users of the system who have pledged to rent their free storage for another user’s to store files. Peers can be created, started, stopped, reconfigured, and even deleted. They expose a set of APIs that enable administrators and applications to interact with the services that they provide

AES

Advance Encryption Standard (AES) is a symmetric key algorithm that supports block length of 128 bit and can have a key size of 128, 192, and 256 bits. The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext. It is based on a substitution-permutation network, also known as an SP network. It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations).

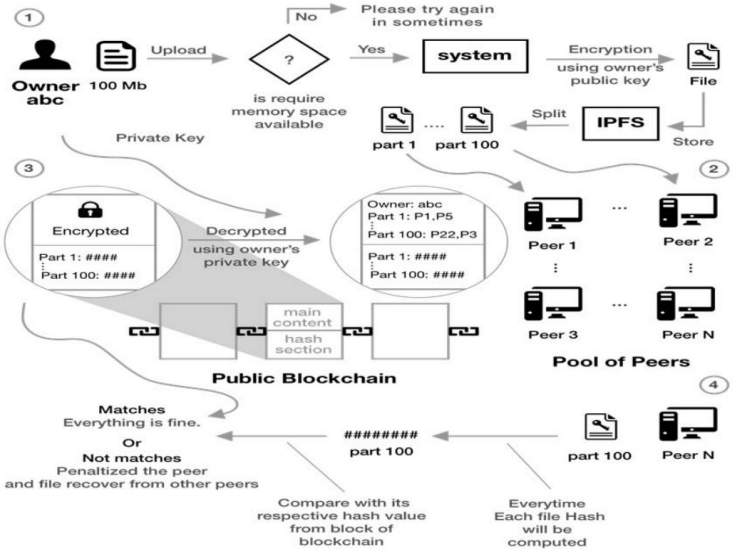
IPFS protocol

IPFS is an open-source peer to peer file transfer protocol. it is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS seeks to create a permanent and distributed web. It does this by using a content-addressed system instead of HTTP's location-based system. Instead of using an location address, IPFS uses a representation of the content itself to address the content. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

III. METHODOLOGY

The user first creates an account on the metamask. The user's account address and wallet balance are fetched in the app through web3.js from the metamask. Users select the file to upload through file picker. System checks for the number of available peers. Further, the AES algorithm uses the user's wallet address as a key and encrypts the uploaded file. A payment dialogue seeks for the user's confirmation. On confirming the payment, the user's file is stored across available peers using IPFS protocol. IPFS then returns a hash value consisting of the path of the file. This path is then mapped with the user's address using a smart contract and gets stored securely in the blockchain. To achieve high availability and reliability of data, the uploaded data is replicated on three peers. For better performance system blacklists peers every time they are unavailable for data retrieval. The proposed system works in four modules shown in fig



A. Uploading of File

User uploads file using the file picker. The system checks the file size and ensures storage availability in the network. The file is uploaded when enough storage is available. Then system performs step B. Users are notified to try again when enough storage is unavailable.

B. Encryption of File

The uploaded file is encrypted using AES 256 bit algorithm. The encryption key is generated using the user's wallet address and randomly generated salt value. This encryption key along with an IV is used to encrypt user's data. This maintains the confidentiality of the user's data.

C. Storing of File Across Multiple Peers

The encrypted file is then divided into blocks of 64KB and sends to different peers across the network with the help of the IPFS protocol. The proposed system uses a private IPFS network to allow registered peers to store the file in the network. The file block is replicated on multiple peer's storages for high availability using the IPFS cluster.

D. Storing of File Across Multiple Peers

IPFS returns a hash value which indicates the path of the file. The hash value along with metadata is mapped with the user's wallet address and is stored in the blockchain using a smart contract. Smart contracts are like agreement and are used to eradicate the need for a third party. They control the transaction between nodes or assets between parties under certain conditions. This is lines of code stored on a blockchain network and are automatically executed when predetermined terms and conditions are met. In our proposed system preconditions for the smart contract to execute are:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

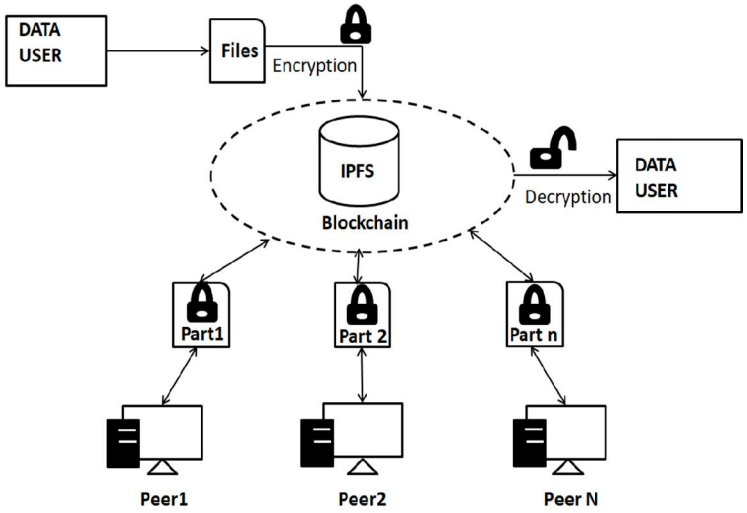
1) Enough Space is available in the network to store files.
2) The user has sufficient wallet balance to pay the peers

Smart Contract to store file details stores all the files details in the structure named File Details and maps this structure with the user's address. It consists of two functions, one to add a new file and another to get the details of the uploaded file.

E. Paying the peers for file storage

Once the file is stored across peers, total cryptocurrency is calculated and is deducted from the user's wallet. This cryptocurrency is first transmitted to the smart contract from the user's wallet. With the smart contract, this amount is distributed to the peers who have stored the user's file. Smart Contract to transfer payment to peers consists of two methods depositFund() and withdraw(). Users can transfer the payment to peers via a smart contract. The user has to first deposit funds into the smart contract using depositFund() function. This payment is then transferred to peers via smart contract by withdraw() function.

IV. SYSTEM ARCHIETECTURE



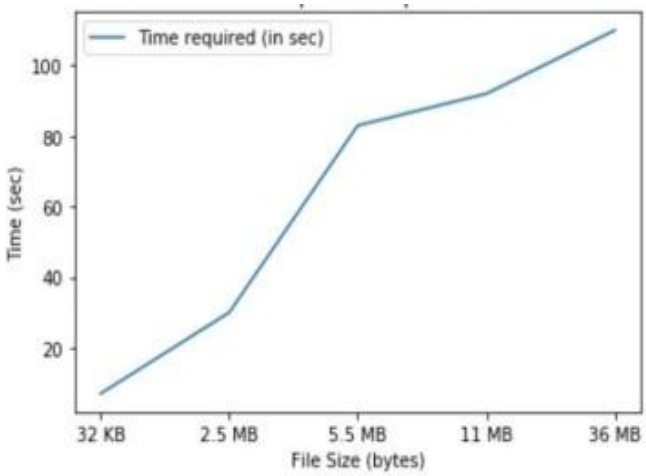
V. RESULT

A. Designed System

To access the system, users first sign up on metamask and login with the registered credentials. Successful login takes users to the home screen for selecting the file to upload. System checks for storage availability based on selected file size. The selected file is encrypted using AES 256 bit algorithm when sufficient storage is available. The system will compute the total cost of storing the file. Once the cost is the calculated system will check if the user's wallet balance is more than the calculated cost. If the user has sufficient balance then he/she is prompt to pay the cryptocurrency to store the file. After a successful payment file is split into blocks and store across peers using IPFS protocol and the corresponding hash value is stored in the blockchain. Once the file is successfully uploaded IPFS returns a hash value indicating the path of the file. This will be mapped with the user's wallet address and will be stored in the blockchain with the help of a smart contract.

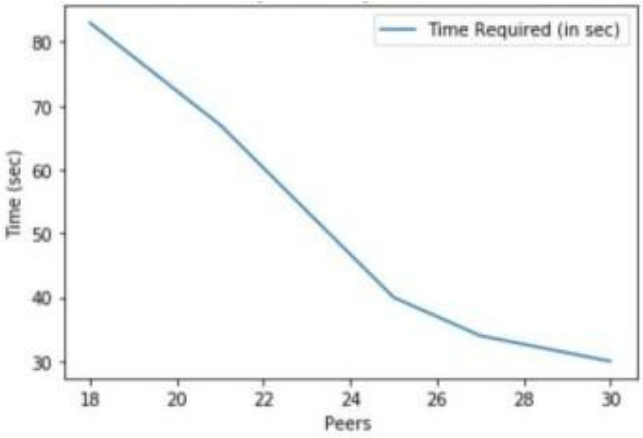
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Time required to upload files



Analysis of time required to upload files

Time required to upload 2.5mb file



The time required to upload 2.5mb file concerning the number of peers

B. Downloading the file from network

First of all select the file from IPFS then enter the hash key to decrypt the file. All the parts get merged from network (peers).AES key is used to decrypt the file, which gives original file as an output.

C. Sharing the file from network

First of all select the file from IPFS then enter the hash key to decrypt the file. All the parts get merged from network (peers).AES key is used to decrypt the file, which gives original file as an output. Then share the decrypted file to other user.

VI .CONCLUSION

The proposed system enhances the security of data by encrypting and distributing the data across multiple peers in the system. Implemented system uses the AES 256bit encryption algorithm to encrypt the data ensuring the confidentiality of the user's data. Encrypted data is then distributed and stored across peers in the network using the IPFS protocol. Our system not only solves the privacy and security concerns of centralized cloud storage but also provides a medium for the peer to rent their under utilized storage and earn cryptocurrency in return thereby, maximizing the storage resource

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

utilization. After conducting research and developing models of decentralized storage logical to draw the following conclusions regarding data storage, providing the highest possible data security:

Secure storage should work in an environment in which the relationship between the parties are not built on trust. Maximum data security is ensured only if no one except the user does not hold the key to access the data. To achieve reliability of the storage system should be decentralized and should share information in an encrypted form between independent storage nodes

Secure storage system must necessarily include monitoring of nodes for failover and verifying data integrity and availability.

REFERENCES

[1]. Zhe, Diao, "Study on Data Security Policy Based On Cloud Storage" 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) IEEE, 2017.

[2]. Nakamoto, Satoshi,"Bitcoin: A peer-to-peer electronic cash system", (2008).

[3]. Zyskind, Guy, and Oz Nathan," privacy: Using blockchain to protect personal data",IEEE Security and Privacy Workshops. IEEE, 2015

[4]. Ruj, Sushmita, et al, "BlockStore: A Secure Decentralized Storage Framework on Blockchain" 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA).

[5]. IEEE, 2018Benet, Juan, "IPFS - Content Addressed, Versioned, P2P File System." 2014.

[6]. Li, Dagang, et al. Meta-Key: "A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture", IEEE Networking Letters 1.1 (2019): 30-33

[7]. Wohrer, Maximilian, and Uwe Zdun,"a Smart contracts: security patterns in the ethereum ecosystem and solidity", International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2018.

[8]. Sum, V. "SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1.01 (2019): 45-54

[9]. Sivaganesan, D. "BLOCK CHAIN ENABLED INTERNET OF THINGS." Journal of Information Technology 1.01 (2019): 1