A Secure File Storage & Retrieval using Blockchain Technology

Yash Ranka[1], Jainam Bagrecha[2], Kavish Gandhi[3], Bhargav Sarvaria[4], Prof. P. M. Chawan[5]

[1,2,3,4]*U. G. Student, Department of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India*
[5]*Associate Professor, Department of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India*

---***---

Abstract - *Data is one of the most critical asset any industry can have. Data can be used to generate relevant knowledge and insights by any organization for its benefits. It is very important that data remains in safe hands, and protecting it with integrity and security is an absolute necessity. With the help of distributed p2p storage and messaging technologies like ethereum swarm and ethereum whisper clubbed with block chain, we propose an efficient data storage DAPP.*

***Key Words*: Blockchain, Swarm, Whisper, Ethereum, File Storage & Sharing, Cryptography, Smart Contracts, Web3, Decentralisation**

1. INTRODUCTION

In this project, we have combined the features of Blockchain and Cryptography to provide an efficient, decentralised and a secure way to store and share files. Cryptography provides a way to conceal our data whereas blockchain is used to make it difficult to modify the stored data and make it available for the user to retrieve it from different hosts. In the proposed technique we have used symmetric key to encrypt our data files. Swarm provides decentralised storage whereas Whisper provides decentralised communication. Communication between users is provided using Ethereum Whisper. It provides user-to-user, encrypted messages.

We encrypt the data file with Advanced Encryption Standard [1] (AES) algorithm, and store it on Ethereum Swarm and share the details with the desired recipient using Ethereum Whisper. The entire transaction is stored using smart contracts to display all the files stored by the user on the Blockchain.

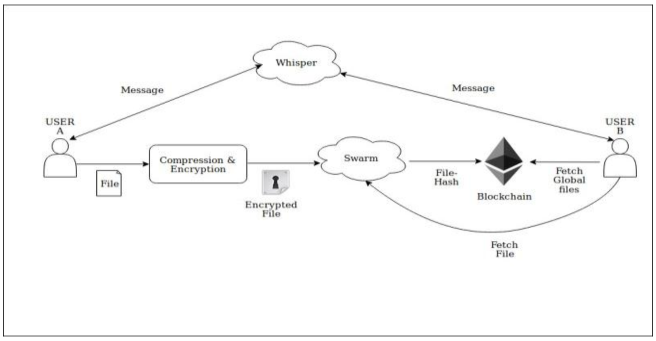

Fig -1: Basic block diagram of file encryption and using blockchain to share

2. LITERATURE REVIEW

2.1 Blockchain [2]

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. It is used to store transactions created by users with fields as input, timestamp, public key, etc. A transaction can't be altered as changing the content of the transactions will change the transaction hash which will cause improper linking of blocks.

2.2 Ethereum [3]

Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality. Ether is a cryptocurrency which is generated by the Ethereum platform. Ether is used to create transactions on the Blockchain. Multiple test networks are available for testing purpose. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network.

2.3 Swarm [4]

Swarm platform provides distributed storage and content distribution service. It divides the file into equal chunks of 4kb and encodes each one of them using randomly generated unique keys, each chunk is then replicated and distributes, providing redundant storage. The encryption and decryption is carried out on user's host machine. It provides storage for DAPPs running on Ethereum. It also provides a means to store DAPP codes. Ethereum provides incentives to Swarm nodes.

2.4 Whisper [5]

Whisper is Packet based messaging system which uses Distributed Hash Tables. It sends asymmetrically encrypted messages. It encrypts its message using the public key of recipient, and thus can only be decrypted by his private key, both provided by the Whisper protocol. It provides a simple API for the DAPPs to connect. It does not store fetched messages, leaving no trail of previous conversation.

3. THE PROPOSED TECHNIQUES

3.1 File Upload Technique

Proposed technique reads the file content, encrypts the data and then uploads it on the Ethereum swarm network. Following are the steps:

1) Read the original data within the file that user wants to upload
2) Encrypt the data of the file by the AES algorithm and using the password given by the user
3) Make a JSON object of the encrypted data and file name
4) Upload the object to the Ethereum swarm network
5) The hash obtained (of the file) is then uploaded on the blockchain, which can be used to retrieve the file from the network.

3.2 File Download Technique

Proposed technique downloads the file content from the Ethereum Swarm network, decrypts it and saves the file. Following are the steps:

1) Take the file hash and password from the user
2) Get the file content using the hash from the swarm network
3) Decrypt the data obtained from previous step using the password (the password used for uploading and downloading the file should be same)
4) Create a new file of the same name and write the decrypted data into the file
5) Save the file locally

3.3 Messaging System

Proposed technique uses Ethereum's Whisper protocol for communication between users. We perform the following steps:

1) Register the user on Whisper and store his identity
2) We run a filter on the protocol to store a user's incoming message
3) When a user wants to send a message, he uses our platform to construct a message addressed to the desired identity
4) The protocol then sends the message and the receiving filter stores it
5) The message is encrypted with the receiver's public key id and therefor can only be decrypted by his private key
6) The received messages are saved on local storage
7) Thus, the message are end to end encrypted and not stored on any central server, thus cannot be accessed by anyone and the encryption makes it even difficult to decipher

4. ADVANTAGES

Advantages of File Storage & Retrieval using Blockchain:

1) Using AES (Advanced Encryption Standard), only the authorized users having the key can view the original file
2) File is sharded, distributed and replicated across multiple nodes, which makes it difficult for the hacker to get access to the whole file
3) Secure communication between users is established to transfer the credentials using decentralized network, thus not storing messages on any central server
4) True ownership of a file is ensured as the transactions on Blockchain cannot be modified
5) Unlimited storage for files is provided

5. CONCLUSION

In this paper, we have proposed a technique to share files and messages using two main modules. One is Ethereum Swarm and another is Ethereum Whisper. We first encrypt the file with AES-CBC algorithm using unique key provided by the user and upload it on Swarm, which further encrypts is using counter mode encryption and shards and replicates files across multiple nodes for easy access. Thus, we provide two levels of security. Ethereum whisper provides a way to send encrypted messages without storing the message on any central server. Whisper uses Asymmetric key encipherment, allowing only the required recipient to decipher the message. Thus, we provide a secure way to store and share files.

REFERENCES

[1] Advanced Encryption Standard, “https://en.wikipedia.org/wiki/Advanced_Encryption_Standard”

[2] Blockchain - Wikipedia , “https://en.wikipedia.org/wiki/Blockchain”

[3] Vitalik Buterin, “Ethereum” , “https://ethereum.org/”

[4] Ethereum Swarm, “https://swarm-guide.readthedocs.io/en/latest/introduction.html”

[5] Ethereum whisper, “https://github.com/ethereum/wiki/wiki/Whisper-PoC-2-Protocol-Spec”