IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Blockchain-Enabled Secure Digital Storage Infrastructure

[1]Omkar Naik, [2]Shubham Sonar, [3]Nishant Kumbhar, [4]Vijay Bhame, [5]Tejaswini Patil
[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor
[1]Department of Computer Engineering,
[1]Dr. D. Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune, India

Abstract: The lack of proper security and encryption in traditional file storage services, raises the concern regarding the privacy of users' data. The Dropbox hack in 2012 and the iCloud leak in 2014 highlighted the vulnerability of such systems, putting at risk the sensitive information of millions of account holders. To address these concerns, this project proposes a Blockchain-based File Storage system that aims to provide stability, privacy, and reliability. The project aims to leverage the robust transparency of Blockchain technology to create a secure file storage system that ensures users' data remains private and protected. The proposed system comprises two key components: a client application that performs data encryption and signing, and a backend Flask server that verifies and validates all signatures and blocks, as well as maintaining network consensus.

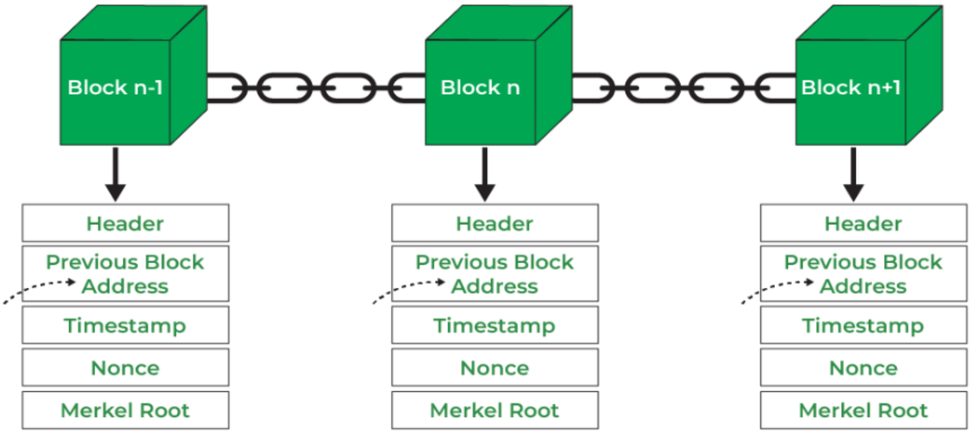
***Keywords* - Blockchain application, File Storage System, AES-256 Algorithm, PoW.**

INTRODUCTION

In the Digital Age, users rely heavily on file storage systems for their data storage needs. Cloud storage solutions like Dropbox, Microsoft One Drive, and Google Drive have become increasingly popular in recent years for data storage and sharing. However, centralized systems are more likely to be attacked, resulting in severe disruption of services. Decentralized storage systems offer several advantages, including overcoming the single-point failure problem and enabling additional benefits like low latency, cheap cost, and the complete removal of confidence in a third party. Online documents have become essential for document verification, and it is crucial to store them in secure file storage systems. However, many file storage services store users' files without properly securing or encrypting them, leading to serious privacy concerns. A Blockchain-based file storage system aims to solve the three major concerns in today's world: stability, privacy, and reliability. This system will allow end-users to interact with the files they upload to the server through a simple user interface. The system consists of a client application responsible for encrypting and signing data, and a Flask server on the backend that verifies and validates all signatures and blocks, ensuring network consensus. Using a hybrid of symmetric and asymmetric key cryptography, this custom Blockchain implementation will enable storing data references, timestamps, performed actions, and cryptographic signatures. With the rapid growth of internet connectivity worldwide, implementing a robust system to counter such security concerns is essential.

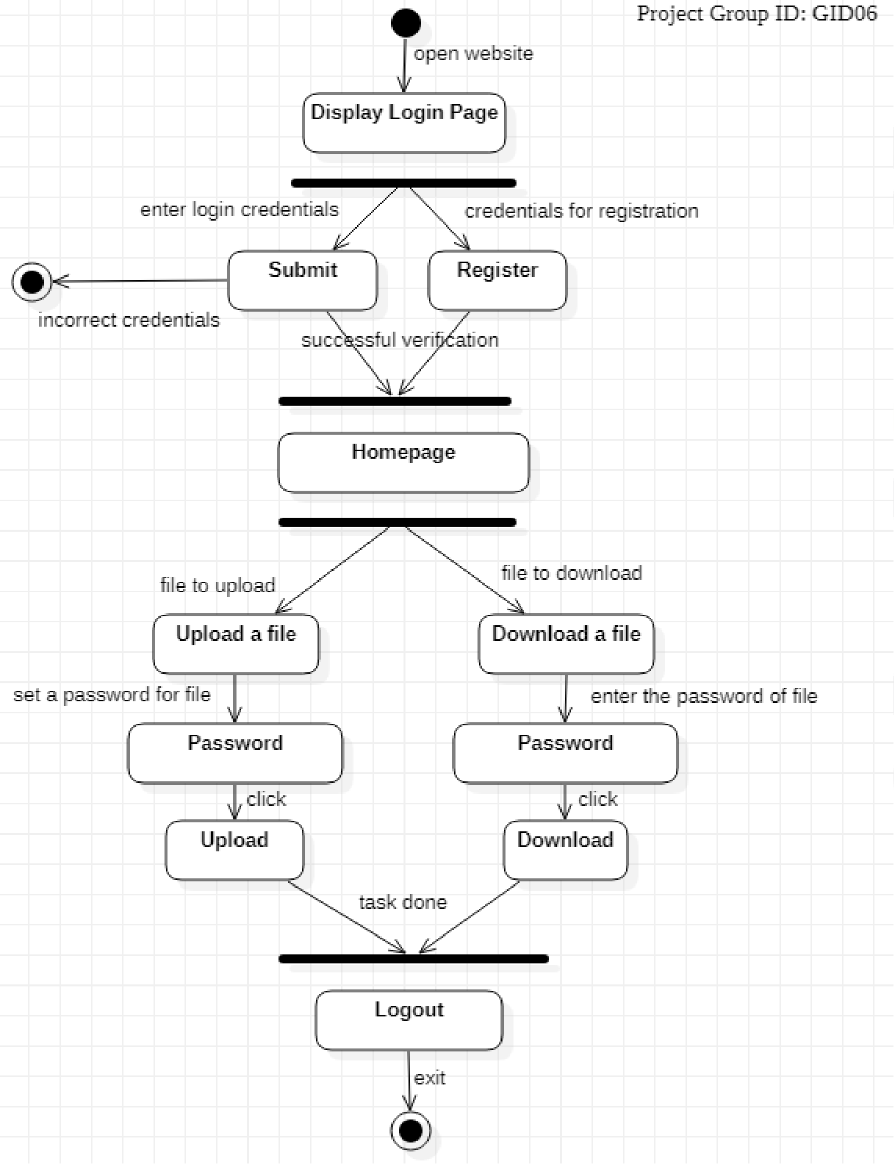
BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed network of digital events that occur and are exchanged by many people who participate. It is built on the Merkle Tree data structure and enables a network of computers to agree on the true state of a distributed ledger at regular intervals. A distributed ledger is a shared, mirrored, and synchronized database that members of a network can access, and each record in a distributed ledger has a unique timestamp and cryptographic signature that uniquely identifies it. It uses a combination of cryptographic algorithms and science theory techniques to ensure the security of the blocks. Any entry in the Blockchain automatically verifies and secures data from previous blocks, rendering tampering virtually impossible.



PROPOSED SYSTEM

This project proposes a private blockchain-based file storage system that aims to address concerns related to stability, privacy, and reliability. The system will have a simple user interface for users to interact with the files they upload to the server. It comprises a client application for data encryption and signing and a Flask server that verifies and validates all signatures and blocks, maintaining network consensus. To guarantee data accuracy, prevent unauthorized data modification, and maintain data credibility, the custom blockchain implementation will employ a combination of symmetric and asymmetric key cryptography. This approach will store data references, timestamps, performed actions, and cryptographic signatures of users. By utilizing this hybrid cryptography method, the blockchain will be resistant to tampering, ensuring that data history remains unaltered.



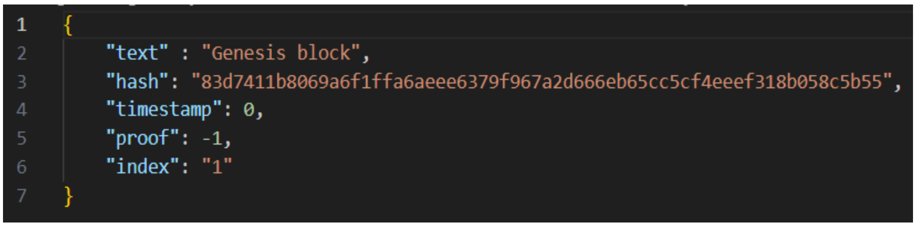
SYSTEM DESIGN

The system includes a privately maintained blockchain server and a web application for user authorization and file access.

4.1 The Blockchain Server

The blockchain server for the system is built using Flask, a micro web framework written in Python. The server includes several functions to manage the blockchain, such as creating a new blockchain, reading existing blocks, and checking the blockchain's integrity. The server also includes an API that can be used to interact with the blockchain, allowing users to create new blocks and fetch existing ones.

At regular intervals, the server runs a function to calculate the proof of work (Pow) for each new block. A proof of work (PoW) is a type of data that is challenging to create but simple to verify, and it must satisfy specific requirements. Generating a proof of work can be a random and low-probability task that typically involves a significant amount of trial and error before achieving a valid proof of work.

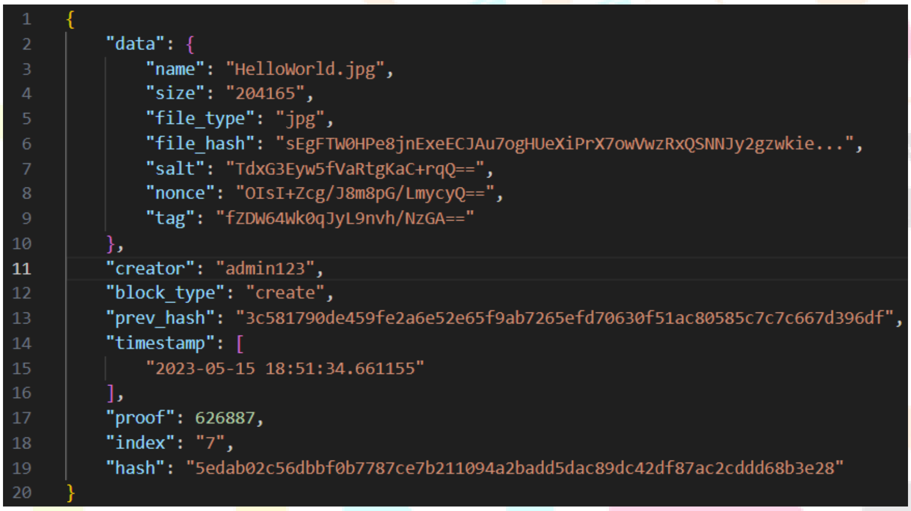


```
{
    "text" : "Genesis block",
    "hash": "83d7411b8069a6f1ffa6aeee6379f967a2d666eb65cc5cf4eeef318b058c5b55",
    "timestamp": 0,
    "proof": -1,
    "index": "1"
}
```

The code block depicted above illustrates the genesis block, which represents the inception of the blockchain.

What is a Genesis block?

A genesis block is the very first block in a blockchain. It serves as the starting point for the entire blockchain network. The genesis block is unique compared to other blocks in the blockchain because it does not reference any previous block, as there are no prior blocks in the chain. Instead, it contains specific data, such as a timestamp, a message, or a reward, that sets the initial parameters and rules for the blockchain. The genesis block is a critical component of a blockchain system because it establishes the foundation of the entire network and sets the stage for subsequent blocks to be added to the chain.



```
{
    "data": {
        "name": "HelloWorld.jpg",
        "size": "204165",
        "file_type": "jpg",
        "file_hash": "sEgFTW0HPe8jnExeECJAu7ogHUeXiPrX7owVwzRxQSNNJy2gzwkie...",
        "salt": "TdxG3Eyw5fVaRtgKaC+rqQ==",
        "nonce": "OIsI+Zcg/J8m8pG/LmycyQ==",
        "tag": "fZDW64Wk0qJyL9nvh/NzGA=="
    },
    "creator": "admin123",
    "block_type": "create",
    "prev_hash": "3c581790de459fe2a6e52e65f9ab7265efd70630f51ac80585c7c7c667d396df",
    "timestamp": [
        "2023-05-15 18:51:34.661155"
    ],
    "proof": 626887,
    "index": "7",
    "hash": "5edab02c56dbbf0b7787ce7b211094a2badd5dac89dc42df87ac2cddd68b3e28"
}
```

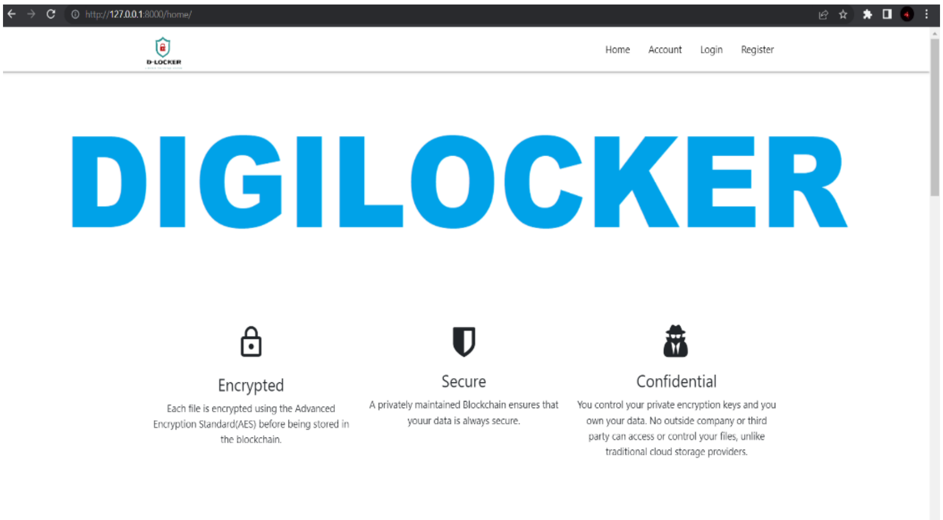
The above code represents a block of data in a blockchain. It contains information about a file, including its name, size, file type, file hash, salt, nonce, and tag. The creator of the block is listed as "admin123", and the block type is "create", indicating that this block was created during the process of adding data to the blockchain. The previous block's hash is listed as "3c581790de459fe2a6e52e65f9ab7265efd70630f51ac80585c7c7c667d39 6df", and the timestamp indicates when the block was created. The "proof" field represents the proof of work required to create this block, and the "index" field indicates the block's position within the blockchain. Finally, the "hash" field represents the unique hash value that identifies this block in the blockchain. This block is an essential component of the blockchain's structure, providing a secure and transparent way to store and verify data.

4.2 Django Web Application

The web application used for the blockchain-based file storage system is Django, a Python web framework that promotes fast development and clean design. The web interface is designed to be user-friendly and allows users to interact with the blockchain, as well as upload and download files. CSS is used as the frontend framework for the web interface.

In this system, OATH is used for user authentication. When a user uploads a file, they select it and enter their private key. To encrypt large data, asymmetric key cryptography is not efficient. Therefore, to encrypt the file, a random 256-bit AES key is generated, and then the key is encrypted using RSA. A new block is created using the encrypted AES key, along with the timestamp, hash of the previous block, user's encoded public key, and file metadata. After that, the block is signed and hashed, serialized into a JSON object, and sent through the API to the backend to be incorporated into the blockchain. On the server side, Flask is used to run the blockchain server, which has a function to create a blockchain, read an existing block, and check its integrity. An API is built into the system to communicate with the blockchain, allowing users to create a new block and fetch a block from the blockchain. At a fixed interval of time, the system runs a function to calculate the proof of work for every new block.

Upon receiving the JSON object, the server undertakes the following steps: it decodes the object utilizing the Base64 decoding technique, then proceeds to recalculate the hash, and finally verifies the signature to ensure that the file's integrity has not been compromised. If the file passes the verification process, the entire object is incorporated into the blockchain where the object remains unchanged and cannot be tampered with, ensuring the security and integrity of the uploaded file.



DIGILOCKER

Encrypted

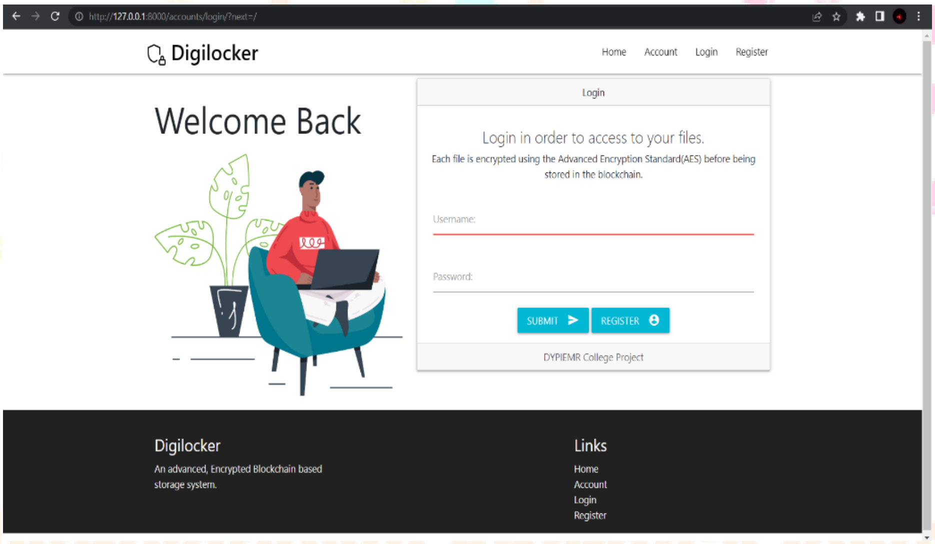
Each file is encrypted using the Advanced Encryption Standard(AES) before being stored in the blockchain.

Secure

A privately maintained Blockchain ensures that your data is always secure.

Confidential

You control your private encryption keys and you own your data. No outside company or third party can access or control your files, unlike traditional cloud storage providers.



Welcome Back

Login in order to access to your files.

Each file is encrypted using the Advanced Encryption Standard(AES) before being stored in the blockchain.

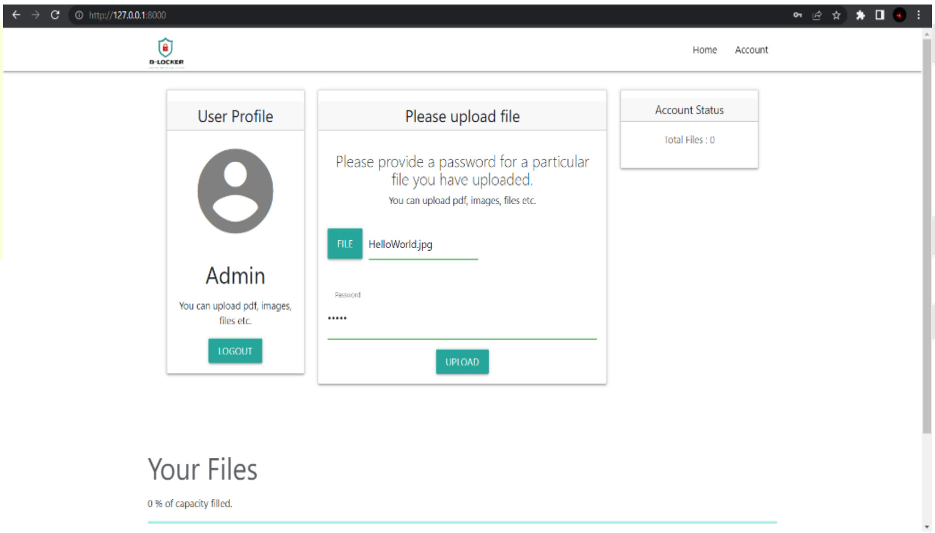
DYPIEMR College Project

Digilocker

An advanced, Encrypted Blockchain based storage system.

Links

Home
Account
Login
Register



User Profile

Admin

You can upload pdf, images, files etc.

Please upload file

Please provide a password for a particular file you have uploaded.

You can upload pdf, images, files etc.

HelloWorld.jpg

Password: •••••

Account Status

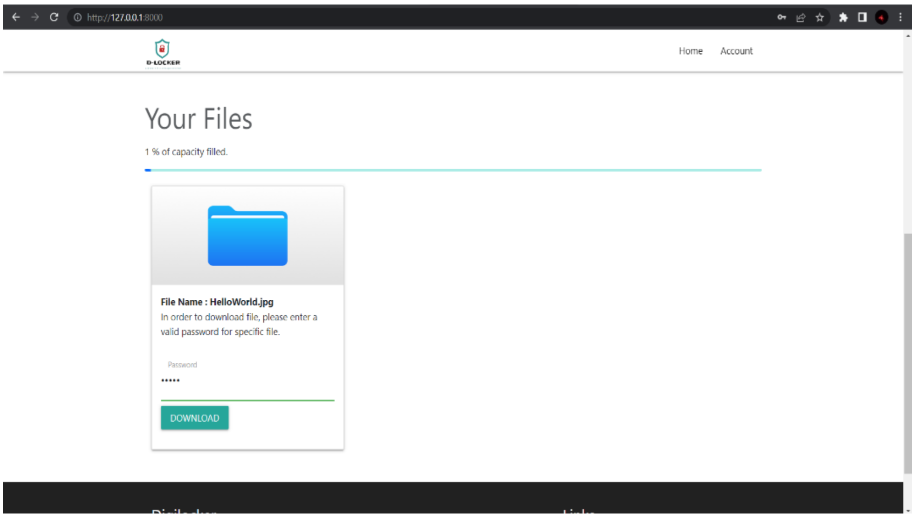
Total Files : 0

Your Files

0 % of capacity filled.

RESULTS

The proposed framework ensures the safe storage and management of user files while maintaining their confidentiality by preventing access by third parties. Even if a file on the blockchain is breached, breaking the encryption to read the contents of the file is very difficult. If the blockchain is tampered with, the system immediately notifies the server administrator to prevent any loss of credibility. The framework also upholds the three critical information security policies: confidentiality, honesty, and availability.



Your Files

1 % of capacity filled.

File Name : HelloWorld.jpg

In order to download file, please enter a valid password for specific file.

Password: •••••

CONCLUSION

A proposed solution is a blockchain-based digital locker in a decentralized application that can securely store personal documents with high availability. The use of blockchain technology makes it challenging for any third party to alter the data history or credibility, ensuring data security. The system also has provisions for verifying documents with confidentiality, access control, data privacy, authenticity, and integrity, making it a robust solution. The proposed solution can be used to store personal documents with a high degree of security and trust.

REFERENCES

[1] Jai Singhal, Ashutosh Bhatia, Ankit Agrawal, Ankit Singh Gautam (2022), "DD-Locker: Blockchain-based Decentralized Personal Document Locker" | DOI:10.1109/ICOIN53446.2022.9687236

[2] Vimal S and Srivatsa S K (2017) "A survey on various file sharing methods in P2P networks" 978-1-5090-4855-7/17/$31.00 ©2017 IEEE.

[3] Menglu Jin, Chi Cui, Gang Yu, Xiaochong Li, Yu Zhang and Li Zeng (2020) "A Blockchain-Based Scheme for Secure Storage and Sharing of Student Digital Profiles" 2020 3rd International Conference on Smart BlockChain (SmartBlock) | 978-1-6654-4073-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/SMARTBLOCK52591.2020.00045

[4] Yogita Sharma, Ayush Agarwalla, Dhananjay Joshi, Divyanshu Prasad (2021) “A Secure Encrypted Digital Storage System Based on Blockchain” Volume:03/Issue:03/March-2021 | e-ISSN: 2582-5208

[5] Yu-Te Wang, Chu-Fei Wu, Shang-Pin Ma, Hsuan-Tung Chen, Shih-Ying Chang and Chun-Sheng Li (2020), "PDAS: A Digital-Signature-Based Authorization Platform for Digital Personal Data" International Computer Symposium (ICS) | 978-1-7281-9255-0/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICS51289.2020.00106.