Using Face Recognized Access for Metamask Integrated Decentralized Cloud Storage

Prof. Pratyasha Pradhan[1], Prof. Oruganti Kalpana[2], Mr. Balakrishna[3], Ms.Sushma Deyannavar[4], Ms. Sushmita[5], Ms.Gowthami S[6]

[1,2] *Professor, CS&E Dept, Proudhadevaraya Institute of Technology, Hosapete*

[3,4,5,6] *Students, CS&E Dept, Proudhadeyaraya Institute of Technology, Hosapete*

***Abstract*—This paper presents a secure, decentralized file storage framework that combines facial-recognition–based biometric authentication with a MetaMask-enabled blockchain environment. The proposed system replaces vulnerable password-based logins with a privacy-preserving biometric module implemented on a Raspberry Pi. After successful authentication, files are stored on the InterPlanetary File System (IPFS), and the associated metadata is recorded on the Ethereum blockchain through a smart contract. This design ensures immutability, transparency, and tamper-proof handling of user files. The system demonstrates how decentralized technologies, Web3 tools, and lightweight biometric processing can be integrated to provide a secure and user-controlled alternative to traditional cloud storage services.**

***Index Terms*—Blockchain, IPFS, Face Recognition, MetaMask, Smart Contract, Decentralized Storage.**

I. INTRODUCTION

Centralized cloud storage systems continue to face major challenges including data breaches, single points of failure, weak password policies, and restricted user ownership of data. With increasing reliance on digital platforms, these limitations significantly impact data integrity, confidentiality, and long-term accessibility. The absence of strong authentication mechanisms further exposes users to credential theft, phishing, and unauthorized access.

To overcome these issues, this work introduces a decentralized storage framework strengthened by biometric authentication. The system eliminates passwords entirely by using face recognition as the primary access control mechanism. The authenticated user can then perform file-related operations through a blockchain-integrated web application. By combining biometric verification, IPFS-based storage, and Ethereum smart contracts, the system ensures security, transparency, and user autonomy.

The objective of this research is to demonstrate a practical, low-cost, and privacy-preserving alternative to traditional cloud storage using modern Web3 technologies. The system also highlights how edge computing and decentralized applications (dApps) can work together to create resilient and tamper-resistant digital infrastructures.

II. LITERATURE REVIEW

.Recent studies highlight the growing use of face recognition and decentralized technologies in secure data management. A Flask-based face authentication system demonstrated high accuracy but was limited by poor lighting conditions and lacked strong cryptographic features. Other works explored decentralized marketplaces using MetaMask and blockchain for secure peer-to-peer interactions. Research on Raspberry Pi-based biometric systems showed the feasibility of lightweight authentication modules for access control.

Studies on blockchain in e-governance and identity management emphasized its capability to prevent tampering, improve transparency, and support decentralized identifiers (DIDs). Deep-learning-based face detection frameworks such as HOG + SVM and CNN-based encoders have also contributed to improving recognition accuracy in real-time environments. Prior literature confirms the potential

of integrating blockchain, biometrics, and decentralized storage, but a unified, user-friendly solution combining all three remains largely unexplored.

III. METHODOLOGY

The proposed methodology integrates biometric authentication with decentralized file handling. The workflow consists of four primary components:

3.1 Biometric Authentication Module

A Raspberry Pi captures user facial data during registration and login. Facial encodings are generated using a deep-learning model after detecting the face using the Histogram of Oriented Gradients (HOG) algorithm. These encodings serve as the user's digital identity.

3.2 Backend and Database Layer

The server validates authentication requests, issues JSON Web Tokens (JWT), and stores user profiles, face encodings, and file metadata in a database.

3.3 Decentralized Storage via IPFS

Uploaded files are stored on IPFS, which assigns each file a unique content identifier (CID). The CID ensures immutability and enables distributed access.

3.4 Smart Contract Integration

An Ethereum smart contract stores file metadata such as owner address, timestamp, and CID. MetaMask is used to authorize blockchain transactions securely.

IV. SYSTEM ARCHITECTURE

The system architecture is composed of hardware, software, and blockchain layers working in synchrony:

4.1 Hardware Layer

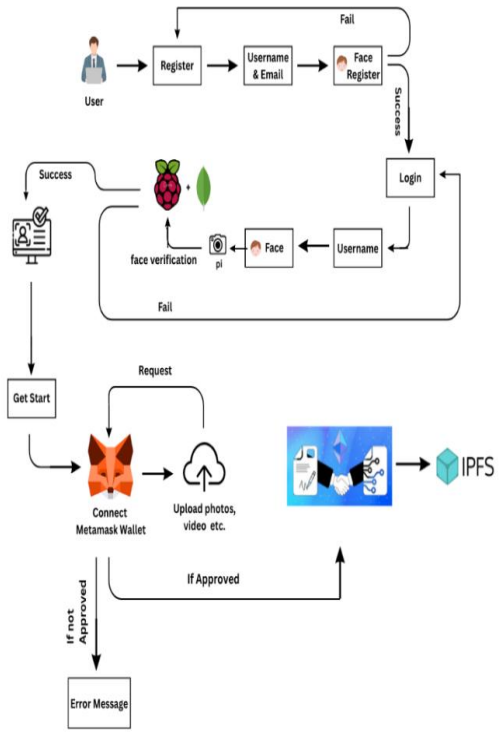
The Raspberry Pi and Pi Camera module perform local biometric processing. This privacy-preserving edge computation ensures that sensitive data never leaves the device in raw form.

4.2 Software Layer

The backend server processes authentication, interacts with IPFS, and communicates with the smart contract. The frontend web interface (developed using Vite and TypeScript) enables users to upload files, check storage logs, and interact with MetaMask.

4.3 Blockchain Layer

Smart contracts deployed through Hardhat maintain a permanent record of file transactions. The tamper-proof nature of blockchain ensures auditability and prevents unauthorized modifications.



4.4 Workflow Overview

1. User verifies identity through Raspberry Pi.
2. Backend issues an authentication token.
3. User uploads a file through the web interface.
4. File is stored on IPFS and returns a CID.
5. CID is stored immutably on the Ethereum blockchain.

V. IMPLEMENTATION

5.1 Face Detection Using HOG

HOG is used as a lightweight and efficient face detection technique on the Raspberry Pi. It extracts

edge and gradient patterns that represent facial structure. The detected face region is then passed to a deep-learning model that generates a 128-dimensional facial encoding.

5.2 Authentication and Token Management
During login, the system compares live encodings with stored encodings to verify identity. Upon successful authentication, the user receives a secure token enabling file operations.

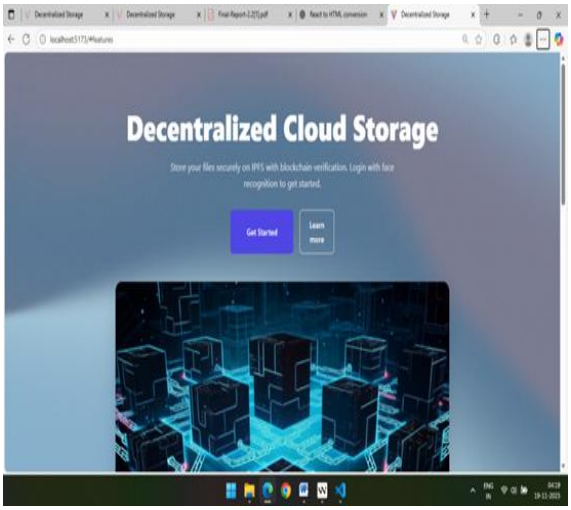
5.3 Storing Files on IPFS
Files uploaded from the frontend are added to IPFS through the backend node. IPFS generates a CID, which acts as the permanent address of the file.

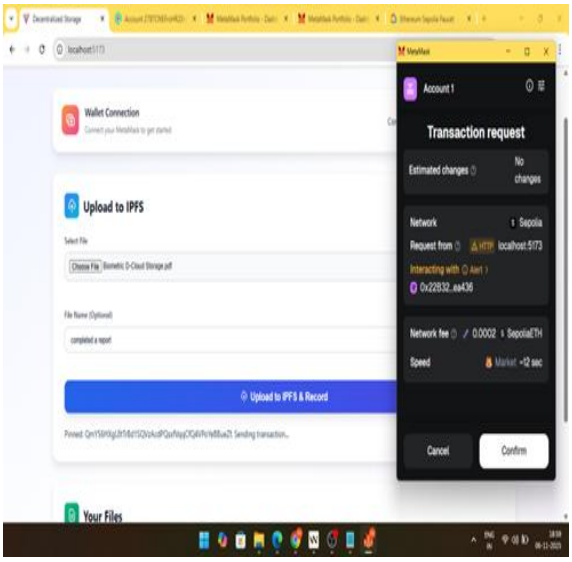
5.4 Smart Contract for File Registry
Each stored file creates a blockchain transaction containing the CID, owner information, and timestamp. MetaMask is used to sign these transactions.

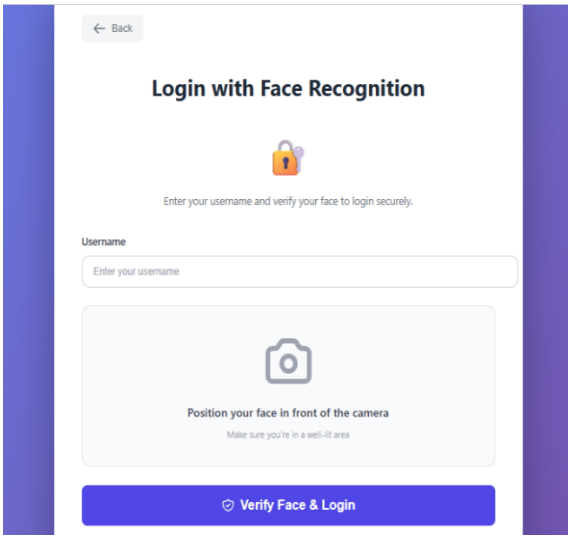
5.5 Frontend Interface
The web interface enables file uploads, CID retrieval, and blockchain record viewing. It provides a simple and user-friendly environment for non-technical users.

VI. RESULTS AND DISCUSSION

The integrated system successfully authenticates users using facial recognition and allows only verified users to access the decentralized storage platform. IPFS storage ensures that files remain accessible even if individual nodes go offline, and the blockchain layer provides an immutable audit trail. The system demonstrates strong security, eliminates password vulnerabilities, and maintains high usability. Results confirm that combining biometrics with Web3 technologies significantly enhances data integrity and user control.







VII. CONCLUSION

In conclusion, this project successfully bridges the gap between cutting-edge technology and practical application, delivering a revolutionary file storage solution that fundamentally reimagines how we approach data security and storage. Through the seamless integration of facial recognition biometrics, blockchain technology, and decentralized storage protocols, this project has created a comprehensive ecosystem that addresses the critical vulnerabilities of traditional centralized systems while maintaining exceptional user experience. The implementation demonstrates that complex Web3 technologies can be made accessible to everyday users without compromising on security or functionality. The project's modular architecture, extensive documentation, and privacy-first approach establish it as both a functional application and a valuable educational resource for the developer community. By eliminating password-based authentication vulnerabilities, ensuring data permanence through IPFS, and providing immutable transaction records via blockchain technology, this system represents the future of secure, user-controlled data storage. The successful deployment of biometric authentication on Raspberry Pi hardware proves that privacy-preserving, edge-computing solutions are not only feasible but essential for protecting user data in an increasingly connected world. This project stands as a testament to the transformative potential of Web3 technologies when thoughtfully integrated to solve real-world problems, paving the way for a new generation of decentralized applications that prioritize user sovereignty, data privacy, and technological innovation.

REFERENCES

[1] Ishita Gupta, Varsha Patil, Chaitali Kadam, and Shreya Dumbre. Face detection and recognition using Raspberry Pi. In 2016 IEEE International WIE Conference 185 on Electrical and Computer Engineering (WIECON-ECE), pages 83–86. IEEE, dec 2016. ISBN 978-1-5090-3745-2. doi: 10.1109/WIECON-ECE.2016.8009092.

[2] Zou, Weiqin, et al. "Smart contract development: Challenges and opportunities." IEEE transactions on software engineering 47.10 (2019): 2084-2106.

[3] Mohanta, Bhabendu Kumar, Soumyashree S. Panda, and Debasish Jena. "An overview of smart contract and use cases in blockchain technology." 2018 9th international conference on computing, communication and networking technologies (ICCCNT). IEEE, 2018.

[4] Meddeb, Houda, Zouhaira Abdellaoui, and Firas Houaidi. "Development of surveillance robot based on face recognition using Raspberry-PI and IOT." Microprocessors and Microsystems 96 (2023): 104728.

[5] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." arXiv preprint arXiv:1906.11078 (2019).