

Decentralized Web Based Identity System Using Blockchain with AI Face Detection

Prof. Rupali R. Jadhav¹, Shruti S. Jadhav², Sushil S. Rankhamb³, Shraddha S. Sadavarte⁴ and Abhijeet S. Sarkate⁵

¹ Professor, ²⁻⁵ Undergraduate Students, Department of Computer Engineering, Zeal College of Engineering and Research, Pune

Abstract

Digital identity systems are widely used in banking, healthcare, education, and online services. Most existing systems rely on centralized databases and password-based authentication, making them vulnerable to cyberattacks, data breaches, and identity theft. This paper presents a decentralized identity authentication system that combines blockchain technology with AI-based face recognition. The system stores a secure cryptographic hash of facial features on the Ethereum blockchain and verifies users through live facial authentication. MetaMask is used for wallet-based identity ownership and transaction validation. By eliminating passwords and centralized storage, the proposed system improves security, privacy, and user control. Experimental results demonstrate successful

registration, authentication, and secure identity management using blockchain and artificial intelligence.

Keywords: Blockchain, Face Recognition, Decentralized Identity, Ethereum, MetaMask, Smart Contracts.

1. Introduction

Digital identity serves as the foundation of modern online services, enabling users to access financial systems, healthcare platforms, educational portals, and government services. Most existing identity management systems rely on centralized databases controlled by organizations or governmental authorities. Although these systems are widely adopted, they suffer from significant security vulnerabilities including data breaches, identity theft, insider attacks, and single points of failure.

The increasing frequency of cyberattacks highlights the limitations of password-based authentication systems. Weak passwords, credential reuse, phishing attacks, and database leaks continue to compromise user accounts across multiple platforms. Furthermore, users often undergo repetitive verification procedures, leading to poor user experience and increased administrative costs.

Blockchain technology offers a decentralized and tamper-resistant alternative for identity management. By distributing trust across a network rather than relying on a central authority, blockchain improves security, transparency, and data integrity. Simultaneously, advances in Artificial Intelligence have enabled reliable biometric authentication using facial recognition technologies.

This research proposes a decentralized identity authentication framework that combines blockchain-based identity management with AI-powered facial recognition. The proposed solution provides passwordless authentication, enhanced privacy, and stronger protection against unauthorized access

while maintaining user ownership of identity credentials.

2. Literature Review

Xiao and colleagues [1] proposed a system that combines blockchain with AI-based facial recognition for identity authentication. Their work demonstrates how blockchain can make identity verification more secure and resistant to tampering. While the approach is promising, it leaves some important issues unaddressed, such as scalability, potential biases in facial recognition, privacy concerns, and the absence of a recovery mechanism for lost private keys.

Alzahab and colleagues [2] explored using fuzzy commitment schemes on blockchain to improve the privacy of biometric data. Their system focuses on fingerprint and iris recognition, providing strong protection for sensitive information. However, it has not been tested in real-world scenarios, and its applicability is limited to just a few types of biometrics.

In a similar vein, Uteyev and Gibadullin [3] proposed a decentralized authentication framework that combines

blockchain and computer vision. Their model shows that blockchain can reduce reliance on centralized authorities, but the lack of performance evaluation and large-scale testing makes it difficult to judge how well it would work in practice.

Agarkar and colleagues [4] focused on self-sovereign identity (SSI) and access control using blockchain, giving individuals full control over their identity data. This represents a meaningful step toward digital autonomy. Still, the system does not integrate biometric authentication and has not been assessed for scalability, which limits its broader use.

Salem and colleagues [5] investigated blockchain-based methods for securely storing and verifying facial biometric data. Their work strengthens data security and minimizes the risk of tampering. However, it only addresses facial recognition and does not consider real-time performance or deployment at large scale.

Ahmed and colleagues [6] examined decentralized SSI systems built on blockchain, aiming to improve privacy, security, and user control over personal

data. Although their work laid an important foundation, it faced challenges related to scalability, regulatory compliance, and limited adoption in real-world applications.

Chandak and Yadav [7] proposed an optimized KYC (Know Your Customer) blockchain system to reduce redundancy in banking verification processes. While their approach improved efficiency in managing customer data, it lacked privacy-preserving mechanisms and was restricted to the banking sector.

Taken together, these studies reveal a clear trend toward using blockchain for decentralized and secure identity management. Despite the progress, common challenges remain, including scalability, privacy protection, real-time performance, and practical deployment. Future research should aim to develop systems that are not only secure and scalable but also user-friendly, combining blockchain, biometrics, and AI while ensuring privacy, regulatory compliance, and broad accessibility.

3. Problem Statement

Current digital identity systems are mostly centralized, controlled by

governments or third-party organizations, and overly dependent on passwords or repetitive KYC processes for authentication. These models create several problems: sensitive data in centralized databases is at risk of breaches, users have limited control over their personal information, and authentication methods are exposed to identity theft and fraud. In addition, password-based systems are inconvenient and insecure, while biometric systems often lack secure storage and can be tampered with without proper protection.

Thus, there is a need for a decentralized identity authentication framework that ensures secure storage, user-controlled access, and reliable biometric verification. By combining blockchain with AI-based face detection, the system can tackle these challenges and deliver a scalable, privacy-focused, and passwordless authentication solution.

4. Objectives

The major objectives of the proposed system are:

- To develop a decentralized identity management platform using blockchain technology.
- To eliminate dependence on traditional password-based authentication.
- To integrate AI-powered facial recognition for user verification.
- To ensure secure and immutable storage of identity records.
- To enhance privacy by storing only cryptographic hashes.
- To provide users complete ownership of their digital identities.
- To reduce repetitive KYC verification processes.
- To improve protection against identity theft and cyberattacks.

5. Proposed System Architecture

The proposed architecture consists of five major components:

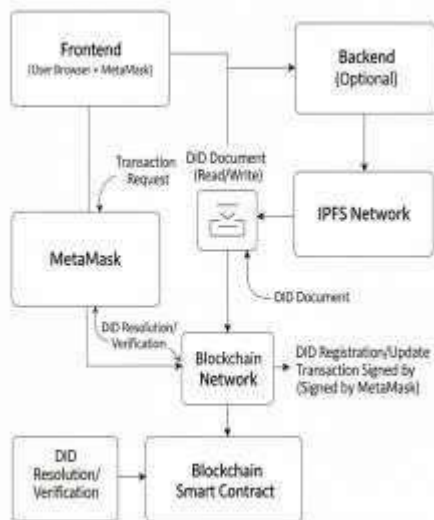
- User Interface (React.js Frontend)
- MetaMask Wallet Integration
- AI Face Detection Module
- Ethereum Smart Contract
- Blockchain Storage Layer

The user accesses the application through a web interface and connects their MetaMask wallet. During registration, facial data is captured using a webcam and processed by the AI module. Facial features are extracted and converted into a SHA-256 cryptographic hash. This hash, along with the user's wallet address, is stored securely on the Ethereum blockchain through a smart contract.

During login, a new facial image is captured and processed. The generated hash is compared against the hash stored on the blockchain. Authentication is successful only when both hashes match

FIGURE 1: System Architecture

6.



Methodology

A. Registration Phase

1. User opens the web application.
2. User connects MetaMask wallet.
3. Webcam captures live facial image.
4. AI module detects facial region.
5. Facial features are extracted.
6. SHA-256 cryptographic hash is generated.
7. Hash is stored on Ethereum blockchain.
8. Registration confirmation is displayed.

B. Authentication Phase

1. User reconnects MetaMask wallet.
2. Live facial image is captured.
3. AI extracts facial features.
4. New hash is generated.
5. Stored blockchain hash is retrieved.
6. Both hashes are compared.

7. Access is granted if hashes match.
8. Access is denied if hashes do not match.

7. Implementation Details

The system was implemented using modern web and blockchain technologies.

Frontend Technologies

- React.js
- Vite
- HTML5
- CSS3
- JavaScript

Blockchain Technologies

- Ethereum Blockchain
- Solidity Smart Contracts
- Hardhat Development Environment

Authentication Technologies

- TensorFlow.js
- Face Detection API
- SHA-256 Cryptographic Hashing

Communication Technologies

- MetaMask Wallet
- Web3.js
- Ethers.js

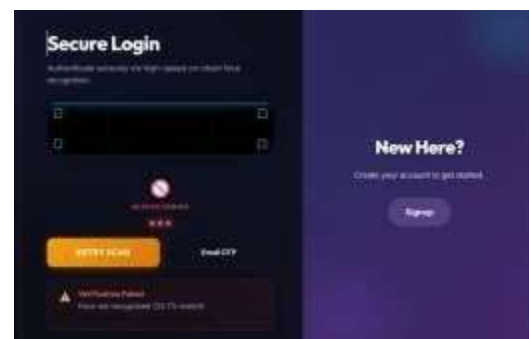
The frontend communicates with the blockchain through MetaMask and Web3 libraries. Smart contracts manage identity registration and verification operations while maintaining data integrity.

8. Experimental Results and Discussion

The developed system was successfully tested in a controlled environment.

User Registration:

Users connected their Ethereum wallet through MetaMask and registered their facial identity. Facial features were extracted successfully and stored as blockchain hashes. Registration was completed successfully for all test users.



Blockchain immutability ensures that identity records cannot be altered after registration.

Phishing Protection

Since the system does not use passwords, phishing attacks become significantly less effective.

Identity Theft Prevention

Authentication requires both wallet ownership and successful facial verification, creating multi-factor security.

Enhanced Privacy

Only cryptographic hashes are stored on-chain, protecting sensitive biometric information.

10. Future Scope

Zero-Knowledge Proof (ZKP) integration.

Multi-biometric authentication.

Mobile application development.

IPFS-based decentralized

storage. Cross-chain identity

interoperability. Government e-

KYC integration.

AI-powered liveness detection.

Quantum-resistant cryptographic techniques.

11. Conclusion

This research successfully demonstrates a decentralized identity authentication framework combining blockchain technology and AI-based facial recognition. By storing only cryptographic facial hashes on the Ethereum blockchain, the system preserves privacy while ensuring secure and tamper-resistant authentication. The integration of MetaMask, smart contracts, and AI-based face verification provides a robust passwordless authentication mechanism. Experimental results confirm the effectiveness of the proposed approach in enhancing security, reducing identity theft risks, and empowering users with control over their digital identities. The system offers significant potential for adoption in banking, healthcare, education, and e-governance applications.

12. References

[1] L. Xiao, L. Zhao, J. Xue, S. Li, W. Li, Z. Dou, and Z. Nie, "Identity Authentication System Based on Blockchain and Artificial Intelligence," 2025.

[2] G. Uteyev and R. F. Gibadullin, "Development of the Decentralized Biometric Identity Verification System Using Blockchain and Computer Vision," in 2024 International Russian Smart Industry Conference (SmartIndustryCon), 2024, pp. 1–6.

- [3] A. A. Agarkar, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, and L. Kulkarni, "Blockchain-aware decentralized identity management and access control system," *Measurement: Sensors*, vol. XX, pp. XX–XX, 2024.
- [4] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-based Biometric Identity Management," *Cluster Computing*, pp. 1–15, 2023.
- [5] N. A. Alzahab, G. Rafaiani, M. Battaglioni, F. Chiaraluce, and M. Baldi, "Decentralized Biometric Authentication using Fuzzy Commitments and Blockchain," *arXiv preprint, arXiv:240*, 2024.
- [6] G. Uteyev and R. Gibadullin, "Development of the Decentralized Biometric Identity Verification System," in *2024 IEEE SmartIndustryCon*, 2024, pp. 1–6.
- [7] Ahmed, M.R., Islam, A.M., Shatabda, S., Islam, S.: Blockchain based identity management system and self-sovereign identity ecosystem: a comprehensive survey. *IEEE Access* 10, 113436–113481 (2022)
- [8] Al-Saggaf, A.A.: A post-quantum fuzzy commitment scheme for biometric template protection: an experimental study. *IEEE Access* 9, 110952–110961 (2021)
- [9] Al-Waisy, A.S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., Nagem, T.A.: A multi-biometric iris recognition system based on a deep learning approach. *Pattern Anal. Appl.* 21, 783–802 (2018)
- [10] Aste, T., Tasca, P., Di Matteo, T.: Blockchain technologies: the foreseeable impact on society and industry. *Computer* 50, 18–28 (2017)
- [11] Arjona, R., Baturone Castillo, M.I.: A post-quantum biometric template protection scheme based on learning parity with noise (LPN) commitments. *IEEE Access* 8, 182355 (2020)
- [12] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.
- [13] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on advances in signal processing*, vol. 2008, pp. 1–17, 2008.
- [14] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern recognition*, vol. 38, no. 12, pp. 2270–2285, 2005.
- [15] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.