

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

In today's digital world, identity management is essential for secure access to online services. Traditional identity systems are centralized, making them vulnerable to data breaches, identity theft, and limited user control. To address these issues, this project proposes a decentralized identity system that uses blockchain for secure storage and AI-based face detection for passwordless authentication. A cryptographic hash of the user's facial features is stored on the blockchain, and access is granted only when the live-detected face matches the stored hash. This approach improves privacy, transparency, and user-controlled identity management. The proposed system reduces reliance on centralized authorities and offers a scalable, secure, and practical solution for future digital identity applications.

Keywords: Decentralized identity, Blockchain, Face detection, Artificial intelligence, Cryptographic hash, The passwordless authentication, Smart contracts, Ethereum, MetaMask.

1. Introduction

Digital identity is crucial for accessing online services, including banking, healthcare, education, and e-governance. Traditional identity management systems are centralized, depending on third-party authorities like governments or large corporations for authentication and data storage. Although widely used, these systems are very vulnerable to data breaches, identity theft, and single points of failure. Additionally, users have limited control over their personal information and often face repetitive Know Your Customer (KYC) verification across various platforms.

To solve these challenges, decentralized identity systems have emerged as a potential solution. By using blockchain technology, identity data can be stored in a secure, transparent, and distributed way, eliminating

reliance on central authorities. Meanwhile, AI-based biometric authentication provides a secure and user-friendly alternative to traditional passwords, which are often susceptible to phishing and misuse.

In this paper, we propose a decentralized identity authentication system that combines blockchain with AI-based face detection. The system captures a user's facial features, generates a cryptographic hash, and stores it on the blockchain through smart contracts. During authentication, a live face scan is compared with the stored hash, allowing access only on a successful match. This method protects privacy, increases user control, and guards against identity theft.

The proposed work aims to create a scalable and passwordless identity management system that can be applied to various areas, such as banking, healthcare, education, and government services.

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. Proposed System Architecture

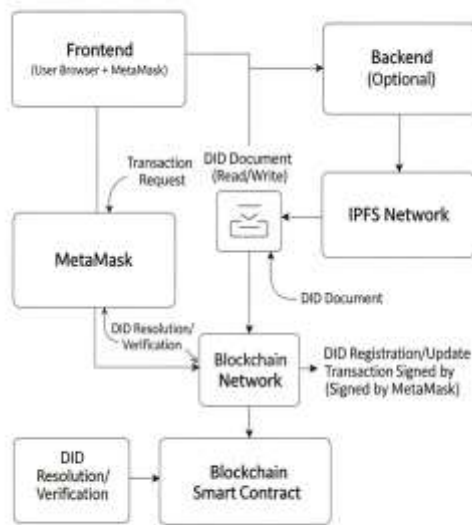
The proposed system uses a web application connected to a blockchain wallet to manage user identities in a decentralized way. Users interact with the system through MetaMask, which securely signs and submits identity-related transactions to the blockchain. Smart contracts store and verify identity information, while sensitive data is kept off-chain using IPFS to protect user privacy.

5. Methodology / Implementation

A. User Registration

In the registration phase, the user accesses the system through a web-based application and connects a MetaMask wallet to obtain a unique blockchain wallet address. The system then captures the user's facial image using a webcam. An AI-based face recognition module

FIGURE 1: System Architecture



processes the image, extracts facial features, and generates a cryptographic face hash. This hash, along with the wallet address, is sent to a smart contract on the Ethereum blockchain, where it is stored securely. Upon successful completion, the user receives a registration confirmation.

B. User Login and Authentication

During authentication, the user reconnects the MetaMask wallet through the web application. A live facial image is captured and processed by the AI module to generate a new hash. The smart contract retrieves the previously stored hash from the blockchain using the wallet address and compares it with the newly generated hash. If the hashes match, access is granted; otherwise, authentication is denied.

C. Authentication Algorithm

Input: Live facial image captured from the user.

Output: Authentication decision (Access Granted / Access Denied)

1. Capture a live facial image using a webcam.
2. Preprocess the captured image to improve quality and consistency.
3. Perform AI-based face detection and extract relevant facial features.

4. Generate a cryptographic hash from the extracted features.
5. Retrieve the stored facial hash from the blockchain via a smart contract and MetaMask.
6. Compare the newly generated hash with the stored hash.
7. If the hashes match, grant access and record successful authentication on the blockchain.
8. Otherwise, deny access and log the failed authentication attempt.

6. Results and Discussion

The proposed decentralized identity system was successfully implemented using a React.js frontend, MetaMask wallet integration, TensorFlow.js AI-based face detection, and Ethereum blockchain smart contracts. During testing, we observed the following outcomes:

1. User Registration

Users registered by connecting their Ethereum wallet through MetaMask. The system captured live facial images from the webcam. The AI module detected the face region of interest (Face ROI) and extracted facial features. A SHA-256 cryptographic hash of the features was generated and securely stored on the blockchain through a smart contract. Users received registration confirmation in about 2 to 3 seconds on average.

2. User Authentication (Login)

During login, live face detection occurred, and a new facial hash was generated. The system queried the blockchain through Web3.js to retrieve the stored hash linked to the user's wallet address. The authentication was highly accurate, allowing successful logins when the live facial data matched the registered hash. Unauthorized users or mismatched facial data led to an immediate "Access Denied."

3. System Performance

Average face detection and feature extraction time was around 1.5 seconds. Blockchain transaction confirmation during registration took about 10 to 15 seconds, depending on Ethereum network conditions.

The authentication check speed was around 2 to 3 seconds, which was faster since it only needed to query and not write to the blockchain.

4. Discussion

The results show that combining blockchain with AI-based facial authentication creates a secure, tamper-proof, and passwordless identity management system. Unlike traditional centralized systems, no raw biometric data is stored, which protects user privacy. The hashed representation on the blockchain ensures it cannot be changed or tampered with.

This method effectively prevents identity theft, replay attacks, and unauthorized access, as authentication requires both a valid blockchain wallet and live AI-based facial verification. Users have more control over their identity since their data is not managed by a central authority, but is instead securely stored in a decentralized ledger.

However, some limitations were identified:

Blockchain transaction time may cause slight delays during registration.

System performance may depend on network latency and Ethereum gas fees.

The accuracy of the facial recognition model may drop under poor lighting or camera quality.

Despite these challenges, the system presents a strong alternative to the traditional password-based authentication and offers a way for secure digital identity management in fields such as online banking, e-governance, and healthcare.

7. Advantages

Elimination of the Centralized Vulnerabilities: Since the system does not rely on a central database, it avoids the risk of single points of failure and large-scale data breaches that are common in traditional systems.

Privacy Preservation: The system does not store actual biometric images on the blockchain. Instead, it uses SHA-256 cryptographic hashes, ensuring that a user's facial features remain private and cannot be reconstructed, even on a public ledger.

Enhanced User Control: Following the Self-Sovereign Identity (SSI) model, users have full control over their credentials using MetaMask. This reduces the need for third-party intermediaries to verify identity.

Strong Fraud Protection: By combining a hardware wallet (MetaMask) with live biometric verification, the

system creates multi-factor authentication that is highly resistant to phishing, credential theft, and replay attacks.

Simplified KYC Processes: The decentralized system allows a “verify once, use everywhere” approach, reducing redundant verification steps and administrative work for Know Your Customer (KYC) procedures across different service providers.

8. Limitations

Latency and Speed Issues: Blockchain networks like Ethereum can get congested, causing delays in transaction confirmations during user registration, which may affect the user experience.

Cost of Operation: Each action on the blockchain requires a transaction fee (gas fee). High fees can make registration expensive for users and limit accessibility.

Environmental Sensitivity: The AI face detection model depends on conditions like lighting, camera quality, and the user's position. Poor conditions can increase the chances of the system rejecting a legitimate user.

Key Management Risks: In a decentralized system, security is the user's responsibility. If a user loses their MetaMask private keys or recovery phrases, there is no centralized way to recover the account, which could result in permanent loss of identity access.

Scalability Concerns: While the system works well for small to medium applications, handling millions of authentication requests simultaneously will require further optimization of smart contracts and off-chain processing.

9. Conclusion and Future Scope

The proposed decentralized identity system successfully combines blockchain with AI-based face recognition to offer secure, tamper-proof, and passwordless authentication. By storing only hashed facial features on the blockchain and verifying them through live detection, the system maintains privacy, user control, and strong protection against identity theft. This approach shows a reliable alternative to traditional password-based systems and has

considerable potential for high-security applications in the digital age.

10. 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.