IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A System For Identity Verification In The Healthcare Sector Blockchain-Enabled

[1]GAYATHRI DEVI T,
[1]Assistant Professor,
[1]Information Technology,
[1]Misrimal Navajee Munoth Jain Engineering College,
[1]Chennai, India

[2]SHEELA O,
[2]Assistant Professor,
[2]Information Technology
[2]Misrimal Navajee Munoth Jain Engineering College,
[2]Chennai, India

ABSTRACT

This project introduces a blockchain-based face identity verification system engineered to bolster security and privacy in digital identity management. The integration of blockchain technology with facial recognition provides a tamper-proof and secure method for verifying user identities. Facial images undergo capture and processing, with identity records stored immutably on a decentralized blockchain network, restricting data access to authorized entities. This blockchain foundation ensures the integrity of identity records, effectively preventing unauthorized modifications and data breaches. This solution offers a transparent and auditable framework for identity verification across diverse applications, including online banking, access control, and digital authentication. The system's efficiency, coupled with blockchain's inherent security and decentralization, establishes a robust platform for contemporary identity verification, significantly mitigating the vulnerabilities associated with conventional systems. This innovative approach promises enhanced user control over personal data and a more secure digital identity ecosystem.

KEYWORDS: Blockchain Technology, Decentralized Identity Management, Electronic Health Records (EHRs), Smart Contracts, Attribute Based Encryption (ABS), Advanced Encryption Standard (AES).

I INTRODUCTION

The Blockchain-Based Face Identity Verification System is an innovative solution designed to revolutionize digital identity management by combining the strengths of facial recognition and blockchain technology. In today's digital world, identity verification plays a critical role in securing access to sensitive services and data across various domains such as banking, healthcare, e-commerce, and government services[1]. However, traditional identity verification systems often rely on centralized databases and physical documents, which are increasingly vulnerable to security breaches, identity theft, data manipulation, and unauthorized access. This system addresses these limitations by introducing a decentralized framework in which user identity data is securely stored and verified using blockchain—a distributed ledger known for its immutability, transparency, and resistance to tampering [2],[3]. Instead of storing raw facial images, the system processes facial features to create a unique digital template. A cryptographic hash of this template is then stored on the blockchain, ensuring that personal biometric data remains private and is not directly exposed or centralized. During the verification process, a live facial image is captured, processed, and hashed. This hash is then compared with the one stored on the blockchain using smart contracts—self-executing code that enforces secure and transparent identity verification. Each verification attempt is recorded immutably, providing auditability and accountability[4],[5]. By integrating blockchain's secure infrastructure with the accuracy and convenience of facial recognition, the system ensures that only authenticated individuals can access protected services. It empowers users with greater control over their

identity information and reduces reliance on vulnerable centralized systems[6],[7]. Additionally, it offers a scalable and efficient approach to identity verification, suitable for both online and physical access scenarios. Overall, the Blockchain-Based Face Identity Verification System presents a robust, user-centric, and future-ready solution to the growing challenges of identity security and digital authentication[8].

II OBJECTIVE

The primary objective of this project is to design and implement a secure and privacy preserving identity verification system that integrates facial biometric recognition with blockchain technology. The system aims to uniquely identify individuals using their facial features, providing a non-intrusive, efficient, and reliable method of authentication. Facial recognition offers a robust biometric foundation due to the uniqueness and stability of facial characteristics, making it ideal for high-assurance identity verification. To ensure data security and prevent unauthorized alterations, the system stores identity information on a blockchain. This distributed ledger provides immutability, transparency, and decentralization, significantly reducing the risks associated with traditional, centralized identity databases. Unlike conventional systems, where identity data is controlled by a single authority, the proposed solution distributes control across the network, eliminating single points of failure and increasing resilience to cyberattacks. Furthermore, the project prioritizes user privacy by avoiding the storage of raw facial images. Instead, it uses cryptographic hashing to convert facial templates into irreversible hashes, which are then securely recorded on the blockchain. This approach ensures that even if the data is accessed, the original biometric information cannot be reconstructed. Ultimately, the system seeks to establish a decentralized, auditable, and secure identity verification framework that enhances trust and safeguards users in digital environments.

III LITERATURE SURVEY

a) SEHR-BC-CHG: Cryptographic Hash Generator with Blockchain

A highly secure framework was proposed by Mubarakali and Basha [9] titled SEHR-BC-CHG (Secure Electronic Healthcare Record – Blockchain with Cryptographic Hash Generator). Their system stores sensitive healthcare records on the cloud using blockchain, applying Discrete Shearlet Transform (DST) for encryption and a Cryptographic Hash Generator (CHG) for transaction authentication. Request validation is optimized using a Hybrid Chaotic Atom Search Optimization Algorithm. The system improves data integrity, confidentiality, and reliability while reducing encryption time by over 20% compared to other models like SEHR-BC-MICEC and SEHR-BC-LFCA. Although focused on medical data, the architecture presents a strong use case for decentralized identity systems.

b) A Hybrid Approach for Approximating the Ideal Observer for Joint Signal Detection

Shrivastava et al. [10] proposed a blockchain-based system utilizing Modified Infinite Chaotic Elliptic Cryptography (MICEC), which combines chaotic neural networks with elliptic curve cryptography to enhance the security and efficiency of data encryption and authentication. This integration strengthens the protection of sensitive information and increases the system's resilience against cyber threats. However, the approach suffers from lower transaction throughput, making it less suitable for real-time applications such as live identity verification. This limitation affects its effectiveness in high-demand, latency sensitive environments where fast and seamless data processing is essential for optimal system performance and reliability.

c)Blockchain-Based Supply Chain Information Sharing Mechanism

Lai et al [3] developed a blockchain-based medical data sharing framework using traceable ring signatures, smart contracts, and distributed key generation to ensure privacy, decentralization, and fine-grained access control. The system utilizes the Inter Planetary File System (IPFS) for scalable and decentralized data storage. While the framework effectively secures sensitive medical information, it is hindered by higher latency and complex signature management. These limitations reduce its practicality for time sensitive applications such as real-time identity verification, where speed and operational simplicity are critical.

d) When Blockchain Meets Supply Chain: A Systematic Literature Review on Current

Development and Potential Applications

Vidhya and Kalaivani [4] proposed a blockchain-based system that employs Lightweight Fused Cryptography (LFC) along with smart contracts to secure medical records. The system operates through six phases, managing the entire data lifecycle including registration, validation, and encryption. It offers high reliability and robust data protection. However, the high latency in accessing encrypted files presents a significant limitation, making it less suitable for time-sensitive applications such as live facial authentication, where rapid data retrieval and processing are crucial.

e) Solving the Sustainable Automobile Production Distribution Joint Optimization in the Physical Internet-Enabled Hyperconnected Order-to-Delivery System

The BACASE-SH model by Arabnouri and Shafieinejad [5] integrates blockchain with certificate-less asymmetric encryption to enhance security in smart healthcare systems. It ensures the availability and integrity of Electronic Health Records (EHRs) while protecting against identity theft and keyword guessing attacks. With low computational overhead, it is well-suited for lightweight identity verification applications However, the model's lower transaction throughput poses a limitation, potentially affecting its scalability and effectiveness in large-scale deployments that require highspeed data processing and response times.

f) Enhancing Blockchain Security Against Data Tampering

Deepa et al. [6] designed a Strict Authentication and Decentralized Storage (SADS) framework, implementing blockchain with SHA-256 for cloud-based EHR systems. Similarly, Agrawal et al. proposed a blockchain and fog computing model using Elliptic Curve Diffie-Hellman (ECDH) and SHA-512, focusing on secure cluster-based data sharing. Both systems demonstrate the potential for decentralized key management and tamper-proof data storage, though each faces trade-offs between encryption time and confidential rate.

IV PROPSED METHODOLOGY

The proposed system is a blockchain-based facial identity verification platform that combines the security, transparency, and decentralization of blockchain technology with facial recognition to provide a private, efficient, and tamper-proof identity solution. It involves capturing and hashing a user's facial features during enrollment, storing the hash on a permissioned blockchain, and verifying identity by comparing the hash of a live facial scan with the stored hash using smart contracts. Facial templates can be securely stored off-chain (e.g., in IPFS) with user-controlled access, ensuring data privacy while maintaining system integrity and auditability.

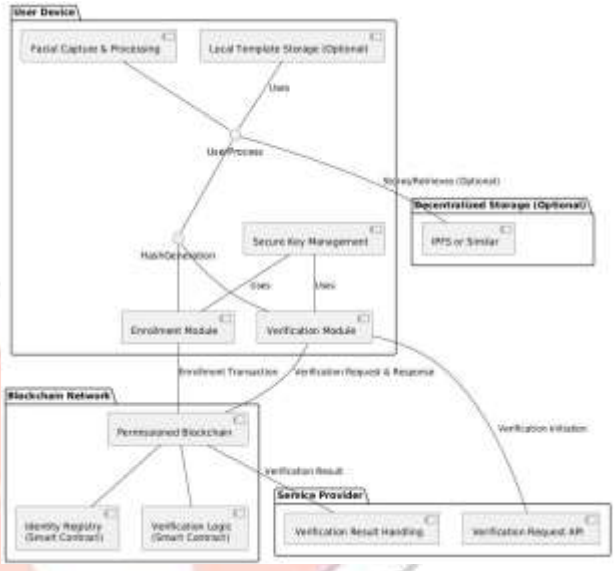

Fig. 1 System Architecture

The architecture diagram illustrates components such as user interfaces, servers, databases, APIs, authentication modules, and third-party services, helping developers and system architects understand the overall structure and data flow of the system to effectively plan deployment and integration.

The system ensures secure, decentralized, and privacy-preserving identity verification by integrating facial recognition with blockchain, requiring users to enrol via facial image capture, hash facial templates, store them on-chain, and verify live inputs against these hashes using smart contracts. It emphasizes secure device-to-blockchain interaction, high accuracy, low latency, strong encryption, user-friendliness, regulatory compliance (e.g., GDPR), and scalability with fault tolerance.

Attribute-Based Encryption (ABE) is employed in the system to enforce fine-grained access control. It is a form of public-key encryption in which both the user's secret key and the encrypted data (ciphertext) are tied to a

set of attributes. Access to the encrypted data is only granted if the attributes associated with the user's key satisfy the conditions defined in the encryption policy. The process begins with key generation, where a trusted authority generates a public key and a master secret key. Based on specific attributes such as a user's role, department, or security clearance level, individual secret keys are issued to users. During the encryption phase, data is encrypted using a defined access policy— for example, "Role = Doctor AND Department = Cardiology". This ensures that only users who meet the criteria specified in the policy are able to decrypt the data. In the decryption phase, when a user attempts to access the encrypted information, their attributes are checked against the access policy. If the attributes match, the user can use their secret key to successfully decrypt and access the data. This mechanism ensures that only authorized users can access sensitive information, thereby enhancing data security and privacy

Advanced Encryption Standard (AES) is used to encrypt facial biometric data before storing it on the blockchain. As a symmetric key encryption algorithm, AES uses the AES (Advanced same key for both encryption and decryption, ensuring efficient and secure data processing. The process starts with key generation, where a random secret key of 128, 192, or 256 bits is created. During the encryption phase, the extracted facial biometric data is encrypted using this AES key, producing ciphertext that is unintelligible without the corresponding decryption key.

V MODULES DESCRIPTION

DATA MODULE

The Data Module is responsible for managing all data-related processes within the system. This includes capturing, preprocessing, storing, encrypting, and retrieving facial biometric data. The core functions of this module are:

• Face Data Capture: Acquires real-time facial images from the user through a camera interface.

•Preprocessing: Normalizes images, extracts relevant facial features, and reduces dimensionality to convert raw images into structured data.

• Encryption: Converts the extracted features into cryptographic hashes (e.g., using SHA256) to ensure that sensitive biometric information is never stored in raw form.

• Blockchain Storage: Securely stores the hashed data on the blockchain ledger, ensuring tamper-proof and verifiable record keeping.

• Data Retrieval: Fetches encrypted data from the blockchain for identity verification during login or access attempts.

This module ensures the integrity, privacy, and availability of user data in a decentralized environment.

PLUGINS MODULE

External systems, frameworks, and utilities. It enhances the system's modularity and The Plugins Module acts as the integration layer that facilitates communication with flexibility.

Its key responsibilities include:

• Blockchain Interface Plugin: Connects the system to the blockchain network (e.g., Ethereum), managing transaction broadcasting, smart contract execution, and ledger updates.

Face Recognition API Plugin: Integrates with third-party or custom facial recognition libraries to process facial images and compare them with blockchain-stored data.

• Security Plugin: Handles cryptographic operations such as hashing, encryption, key generation, and digital signatures.

• User Interface Plugin: Manages dynamic user interaction elements, including login forms, verification prompts, and access control interfaces.

The Plugins Module ensures the system remains scalable, extensible, and adaptable to future technological advancements.

VI IMPLEMENTATION

Fig. 2 User Interface-1

Figure 2 shows the first user interface of the system. User can enter the password and click the 'Go' button.

Fig. 3 User Interface-2

Figure 3 shows the second user interface of the system. Select the size of the picture. After that, face is scanned and the name is also entered.

Fig. 4 User Interface-3

Figure 4 shows the third user interface of the system. After scanning the face and entering the name, the training is completed and the data is stored in the database.

VII CONCLUSION

This paper proposes a blockchain-based facial identity verification system that leverages hashed biometric data stored on a decentralized ledger to enhance security, privacy, and user control. By eliminating centralized vulnerabilities and using smart contracts for verification, the system supports practical applications such as online banking and access control. While technical and regulatory challenges remain, the solution offers a secure, scalable, and privacy-preserving alternative to traditional identity verification methods.

VIII FUTURE WORK

Future enhancements for the proposed blockchain-based facial identity verification system include integration with Self-Sovereign Identity frameworks, advanced liveness detection, privacy-preserving techniques, cross chain interoperability, zero-knowledge proofs, improved user experience, decentralized recovery, hardware security integration, dynamic risk assessment, AI-driven fraud detection, and participation in standardization efforts for broader adoption and security.

IX REFERENCES

1.D. Shakhbulatov, J. Medina, Z. Dong, and R. Rojas-Cessa, "How Blockchain Enhances Supply Chain Management: A Survey," IEEE Open Journal of Computational Science, Volume.1, pp. 230–249, 2020.

2. D. Jie, W. Qingguo, Z. Haifeng, and Z. Xuejing, "Research on Supply Chain Management of Complex Product System Based on Blockchain," Journal of Systems Engineering and Electronics., Volume.35, no. 6, pp. 1530–1541, Dec. 2024.

3. S.-J. Hsiao and W.-T. Sung, "Blockchain-Based Supply Chain Information Sharing Mechanism," IEEE Access, Volume.10, pp. 78875–78886, 2022.

4.S.E.Chang and Y. Chen, "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications," IEEE Access, Volume. 8, pp. 62478–62494, 2020.

5. Y. Xue, S. Ji, G. Zhu, and P. Zhao, "Solving the Sustainable Automobile Production Distribution Joint Optimization in the Physical Internet-Enabled Hyperconnected Order-to-Delivery System by I-NSGAIII," IEEE Access, Volume.11, pp. 7471–7494, 2023.

6. U. Islam et al., "Enhancing Blockchain Security Against Data Tampering: Leveraging Hybrid Model in Multimedia Forensics and Multi-Party Computation for Supply Chain Data Protection," IEEE Access, Volume.12, pp. 111007–111020, 2024.

7. K. Li, W. Zhou, H. Li, and M. A. Anastasio, "A Hybrid Approach for Approximating the Ideal Observer for Joint Signal Detection," IEEE Trans. Med. Imaging, Volume.41, no. 5, pp. 1114–1124, May 2022.

8.S.Oğuz, G. Alkan, B. Yilmaz, and C. Kocabaş, "The Use of Blockchain Technology in Logistics and Supply Chain Management (SCM): A Systematic Review," IEEE Access, Volume.12, pp. 166211–166224, 2024.