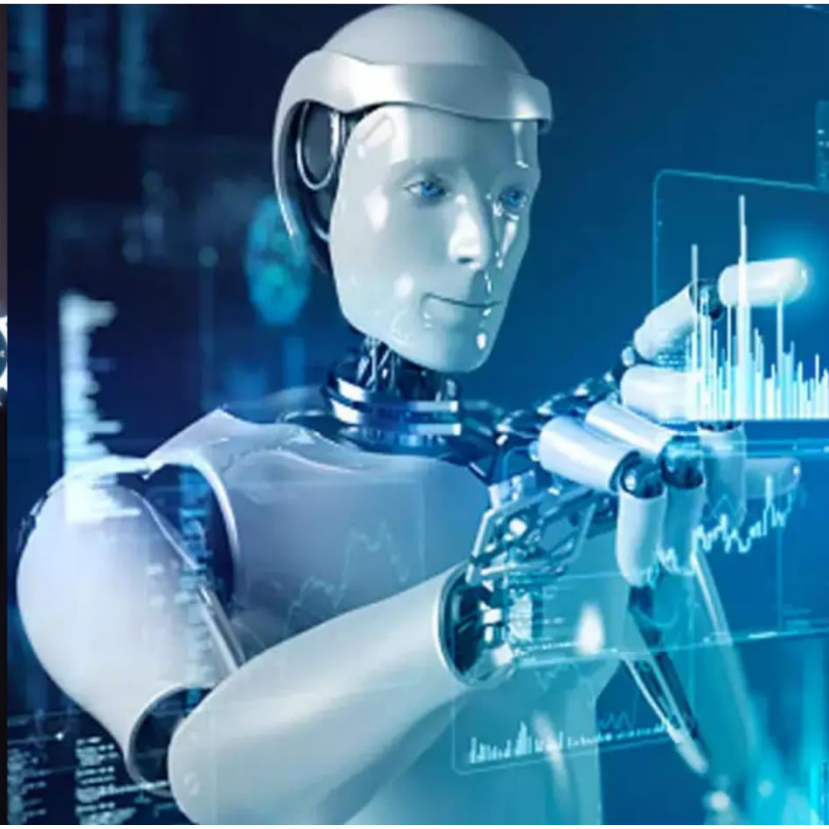
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.699**

**Volume 15, Issue 2, February 2026**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502088|

# Blockchain Based Identity Verification System

**Jenisha M[1], Abinaya S[2], Poorna Seetha B[2]**

Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Nagercoil, Tamil Nadu, India[1,2]

Associate Professor, Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Nagercoil, Tamil Nadu, India[3]

**ABSTRACT:** Proposal of a biometric-based identity verification system integrated with blockchain technology. Facial recognition is used as the biometric method. During registration process a reference image is captured and securely stored. In authentication process Device camera automatically activates. Captures a live photo of the user. Compares the live image with the stored reference using biometric matching algorithms. Successful verification grants access to a blockchain backed digital identity. Blockchain ensures tamper-resistant recordkeeping and decentralized user control. Incorporates liveness detection to mitigate spoofing attacks.

Growing Need for Secure Digital Identity – In today's digital world, identity theft, fraud, and unauthorized access are major concerns in online platforms, e governance, and financial services. Limitations of Traditional Methods – Passwords, PINs, and centralized databases are vulnerable to phishing, hacking, and data breaches. Role of Biometrics – Biometric authentication (face, fingerprint, iris) offers unique and difficult-to-forge identity markers, enhancing security. Blockchain as a Solution – Blockchain provides decentralization, immutability, and transparency, making it ideal for tamper-proof identity management.

**KEYWORDS:** Blockchain-based identity verification, Biometric authentication, Facial recognition, Liveness detection, Decentralized identity (SSI / DIDs), Smart contracts, Biometric template hashing, Off-chain storage / IPFS, Privacy preserving authentication, Verifiable credentials, Authentication audit trail / immutability, Face Net / CNN (deep learning), Enrolment & authentication workflow, Revocation & credential management, KYC / regulatory compliance.

## I. INTRODUCTION

In today's digital world, identity theft, fraud, and unauthorized access are major concerns in online platforms, e governance, and financial services. Limitations of Traditional Methods are Passwords, PINs, and centralized databases are vulnerable to phishing, hacking, and data breaches. Biometric authentication (face, fingerprint, iris) offers unique and difficult-to-forge identity markers, enhancing security. Blockchain provides decentralization, immutability, and transparency, making it ideal for tamper-proof identity management. Integration of Biometrics with Blockchain is by combining biometric authentication with blockchain, we can create a secure, privacy-preserving, and user controlled digital identity system.

## II. LITERATURE REVIEW

Digital identity verification has been an active area of research due to the increasing reliance on online services and the growing number of security breaches in centralized authentication systems. Traditional identity management systems primarily depend on passwords, identity cards, or centralized databases, which are vulnerable to data breaches, identity theft, and unauthorized access. Several studies have highlighted that centralized storage of sensitive identity information creates a single point of failure, making such systems unsuitable for modern security requirements. Bio metric authentication has been widely explored as a more secure alternative to traditional methods. Jain et al. (2021) emphasized that biometric systems provide higher security because biometric traits are unique, non-transferable, and difficult to forge.

## III. METHODOLOGY

This project adopts a developmental and experimental research methodology to design, implement, and evaluate a blockchain-based identity verification system integrated with facial recognition and liveness detection. The

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502088|

methodology focuses on building a functional prototype and assessing its performance in terms of security, accuracy, and usability

● System Design Approach

The system is designed using a layered architecture consisting of three main components: the application layer, the biometric processing layer, and the blockchain layer. The application layer provides a user interface through a web or mobile application for user registration and authentication. The biometric processing layer handles facial recognition and liveness detection using deep learning algorithms.

● Biometric Data Collection and Processing

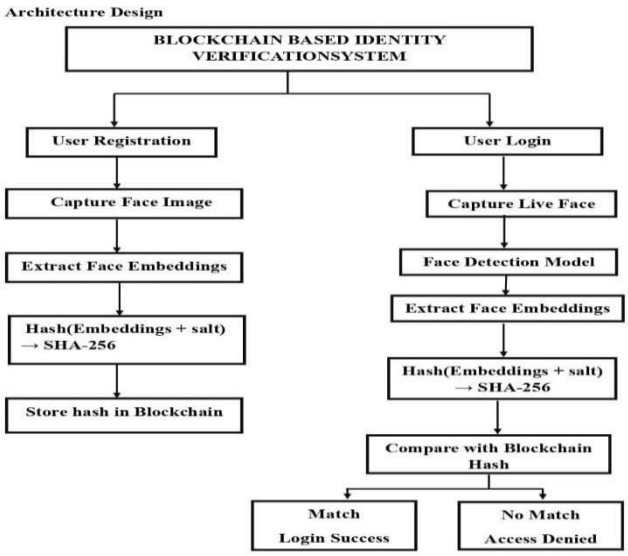
During the registration phase, facial images are captured using a device camera. The captured images undergo pre-processing steps such as face detection, normalization, and feature extraction. Deep learning–based facial recognition models are used to extract discriminative facial features and generate a biometric template. To preserve user privacy, raw facial images are not stored.

● Liveness Detection Mechanism

To prevent spoofing attacks, liveness detection techniques are integrated into the authentication process. Both passive and active liveness detection methods are employed, including texture analysis, motion detection, and user actions such as blinking or head movement.

## IV. ARCHITECTURE

A Blockchain-Based Identity Verification System is a secure authentication framework that combines biometric facial recognition with blockchain technology to verify a user's identity. During registration, a user's face is captured and converted into unique numerical features (face embeddings), which are then hashed with a salt using SHA-256 and securely stored on the blockchain. The original face image or raw biometric data is never stored.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502088|

## V. IMPLEMENTATION

The implementation of the Blockchain Based Identity Verification System translates the proposed architecture into a functional and secure working model. The system integrates facial recognition, liveness detection, and blockchain technology to provide decentralized and tamper-proof identity verification. The implementation is carried out in a modular manner to ensure scalability, security, and ease of maintenance.

- Registration Module

The registration module is responsible for enrolling users into the system. During registration, the user accesses the application through a secure web or mobile interface. The device camera captures a facial image, which is preprocessed to enhance image quality and normalize facial features. Deep learning–based facial recognition algorithms extract distinctive facial features and generate a biometric template.

- Authentication Module

The authentication module verifies the user's identity during login or access requests. When authentication is initiated, the device camera captures a live facial image in real time. Liveness detection techniques are applied to confirm that the image originates from a live person and not from a spoofing medium such as a photograph or video

- Blockchain and Smart Contract Implementation

Blockchain technology is implemented to provide decentralization, immutability, and auditability. Smart contracts deployed on the blockchain manage user registration, authentication validation, and identity revocation. Only the cryptographic hash of the biometric template and relevant metadata are stored on-chain, ensuring privacy protection

- Backend and Data Management

The backend server acts as an intermediary between the application, biometric processing modules, and the blockchain network. It handles API requests, encryption, template management, and communication with smart contracts.

## VI. RESULTS & DISCUSSION

This section presents the results obtained from the implementation and evaluation of the Blockchain Based Identity Verification System and discusses its effectiveness in terms of authentication accuracy, security, privacy, and system performance.

The facial recognition module demonstrated high accuracy in identifying legitimate users. The system was able to successfully match live facial images with the stored biometric templates even with variations in facial expressions, lighting conditions, and camera angles. The False Acceptance Rate (FAR) was observed to be low, indicating strong resistance to unauthorized access, while the False Rejection Rate (FRR) remained minimal, ensuring a smooth user experience for legitimate users.

1.Welcome page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

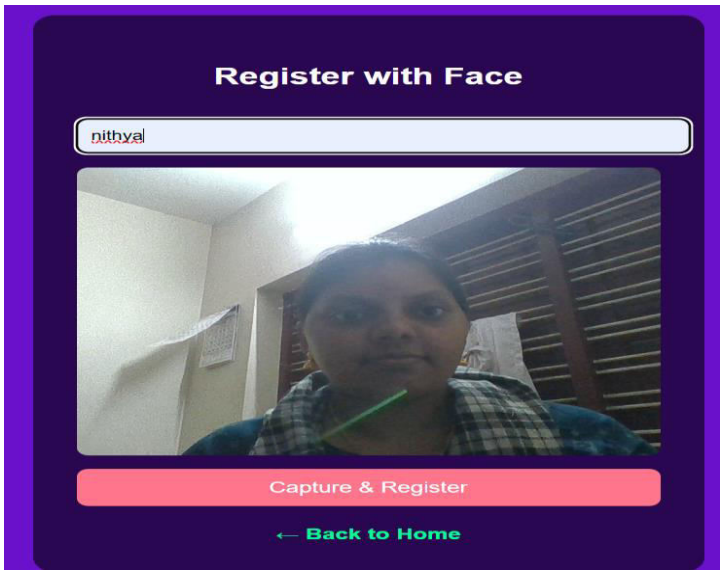
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

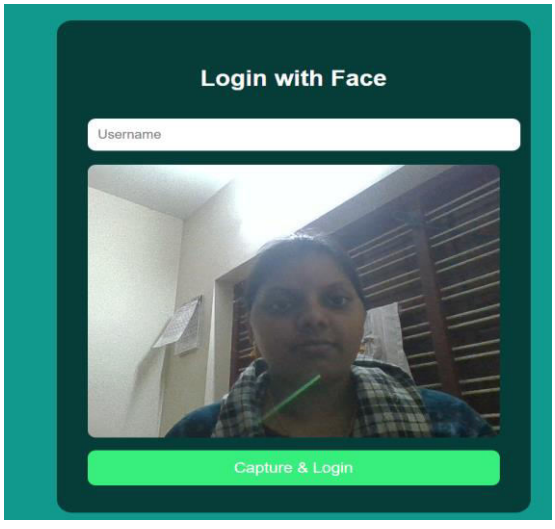
|DOI: 10.15680/IJIRSET.2026.1502088|

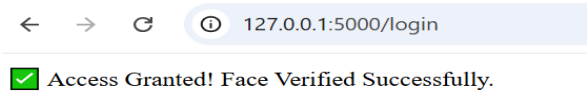
2.Register page





3.Login page



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502088|

## VII. CONCLUSION

The development of a biometric-based blockchain identity verification system represents a significant advancement in digital identity management, combining the strengths of facial recognition technology and blockchain security. The system ensures that users can verify their identities securely, reliably, and efficiently, while minimizing the risk of identity theft, fraud, and unauthorized access.

This project successfully designed and implemented a Blockchain Based Identity Verification System that integrates facial recognition, liveness detection, and blockchain technology to address the security and privacy limitations of traditional identity authentication methods.

## REFERENCES

1)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.
2)P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), pp. 511–518, 2001.
3)F. Schroff, D. Kalenichenko and J. Philbin, "Face Net: A Unified
Embedding for Face Recognition and Clustering," Proceedings of the IEEE - Conference on Computer Vision and Pattern Recognition (CVPR), pp. 815– 823, 2015.
4)Z. Chingovska, A. Anjos, and S. Marcel, "On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing," IEEE International Conference on Biometrics, pp. 1–7, 2018.
5)S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[Online]. Available: https://bitcoin.org/bitcoin.pdf
6)G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Yellow Paper, 2014.
7)G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy:
Using Blockchain to Protect Personal Data," IEEE Security and Privacy Workshops, pp. 180–184, 2015.
8)F. Ferdous, R. Chowdhury, and M. O. Alassafi, "In Search of Self Sovereign Identity Leveraging Blockchain Technology," IEEE Access, vol. 7, pp. 103059– 103079, 2019.
9)A. Liu, X. Zhang, and J. Chen, "Blockchain-Based Secure Biometric Authentication System," Future Generation Computer Systems, vol. 109, pp. 304–316, 2020.
10)P. Sicari, A. Rizzardi, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146– 164, 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details