IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 13, Issue 2, April-May 2025
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Centralized Administration Using Unique Identification for Individuals

Nadera Banu A[1], Dr. K. Kalai Kumar[2], Neshali Kannan[3] and Dhanushiya K[4]

[1] Department of Artificial Intelligence and Data Science, DMI College of Engineering, Chennai, Tamil Nadu 600123, India
naderahussain4@gmail.com

[2] Department of Artificial Intelligence and Data Science, DMI College of Engineering, Chennai, Tamil Nadu 600123, India
kalaikumar23@gmail.com

[3] Department of Artificial Intelligence and Data Science, DMI College of Engineering, Chennai, Tamil Nadu 600123, India
neshalikannan77@gmail.com

[4] Department of Artificial Intelligence and Data Science, DMI College of Engineering, Chennai, Tamil Nadu 600123, India
dhanushiyakannan24@gmail.com

Abstract

The Centralized Administration Using Unique Identification for Individuals project establishes a comprehensive, unified, and secure identity system integrating personal, educational, financial, and legal records from birth to death. Replacing multiple documents such as Aadhaar, PAN, medical records, and travel tickets, it ensures seamless authentication and accessibility across sectors. Utilizing multi-modal biometrics (fingerprint, iris, facial recognition), AI-driven encryption, and blockchain-based security, it enhances fraud prevention, data integrity, and identity verification. The system improves governance efficiency, reduces redundancy, and provides universal accessibility, benefiting newborns, the elderly, and persons with disabilities. Real-time authentication, automated updates, and emergency medical access further streamline services. Aligning with SDGs 16, 9, and 3, this initiative fosters technological innovation, efficient service delivery, and universal legal identity, bridging the gap between technology and governance. This project lays the foundation for a safer, digitally empowered India.

Keywords: *Unique Identification System, Biometric Authentication, Blockchain Security, AI Driven Encryption, Seamless Authentication, Universal Identity Solution, Centralized Database System, Data Integrity and Security, Sustainable Development Goals (SDGs).*

1. Introduction

In the digital era, identity verification and management have become crucial for seamless access to public and private services. Traditional systems relying on multiple identification documents often lead to inefficiencies, fraud, and administrative burdens. The need for a unified and secure system that consolidates all essential records, including financial, medical, legal, and personal information, is more pressing than ever. The Centralized Administration Using Unique Identification for Individuals serves as the backbone, while the Janmitra Card functions as the physical medium through which users interact with the system.

1.1 Background of the Problem

Currently, India uses a number of identity documents, including voter ID, Aadhaar, PAN, and other state-issued records, which leads to administrative redundancies. Inefficiencies, identity theft, and trouble confirming people's qualifications are the outcomes of this fragmentation. Data breaches and privacy issues have increased as a result of the absence of a centralized, impenetrable identity system [1].

1.2 Importance of Unique Identification in Governance

By facilitating precise identity verification, lowering fraudulent activity, expediting service access, and increasing overall efficiency, a strong unique identification system strengthens governance. By combining blockchain-based authentication, AI-driven encryption, and multi-modal biometrics, a single, verifiable credential for all identity-based services can be created, removing duplication and increasing transparency [2].

1.3 Objectives and Scope of the Project

The following are the main goals of this study: to create a centralized, safe identity system for all Indian citizens. to use a single, widely recognized ID in place of several identity documents. to incorporate biometric authentication (facial recognition, iris, and fingerprint) in order to prevent fraud.to facilitate travel authentication, legal paperwork, medical records, and financial transactions.to make it possible to track identity misuse in real time using AI-driven monitoring.to implement an OTP-based authentication system in order to increase the security of verification .To provide emergency access in dire circumstances, like medical crises, where a user's card can be accessed by verified nominees (parents or legal guardians, for example) under stringent security measures .This system will be accessible to people in places with inadequate digital infrastructure because it will operate both online and offline.

1.4 Alignment with Sustainable Development Goals (SDGs)

The Sustainable Development Goals (SDGs) of the UN are in line with this initiative: SDG 16 (Peace, Justice, and Strong Institutions): lowering fraud and guaranteeing everyone's legal identity. Utilizing cutting-edge technologies for identity verification is part of SDG 9 (Industry, Innovation, and Infrastructure). Digital medical records should be made available for easy access to healthcare in order to achieve SDG 3 (Good Health and Well-Being) [3].

2. Related Works

Globally, a number of identity management systems that incorporate blockchain, encryption, and biometrics have been developed. This section examines the shortcomings of the current solutions and shows how the suggested system outperforms them.

2.1 Aadhar–India's biometric Identification system

Over 1.3 billion people are covered by the largest biometric identity system in the world, Aadhaar, which was introduced by the Unique Identification Authority of India (UIDAI). For authentication, it makes use of iris and fingerprint recognition. However, Aadhaar has experienced vulnerabilities in centralized storage, data leaks, and privacy issues [4]. The proposed system, in contrast to Aadhaar, combines blockchain technology with AI-driven security to guarantee data integrity and decentralization.

2.2 Blockchain-based Identity systems

Blockchain technology is used in a number of decentralized identity management models to store identities in an unchangeable and impenetrable manner [5]. Full decentralization, however, may result in problems with cost and scalability. The suggested system strikes a balance between tamper-proof security and accessibility by combining blockchain security with centralized efficiency.

2.3 International Digital Identity Initiatives

Digital identity systems that combine smart cards and online authentication have been put into place in nations like the UK and Estonia [6]. However, multi-modal authentication and biometric security are frequently missing from these systems. By combining secure offline authentication with fingerprint, iris, and facial recognition, the Janmitra Card overcomes this restriction. By combining blockchain, AI-driven fraud detection, and multi-modal biometrics into a single, high-security identity system, this paper builds on earlier research.

3. Proposed Approach

The proposed system, Janmitra card, integrates identity management from birth to death, ensuring secure and seamless verification across various sectors such as finance, healthcare, government, and public services. This section describes the core mechanisms and technological components that make the system robust and scalable.

3.1 Unique ID Generation Mechanism

Unlike Aadhaar's randomly assigned numbers, the proposed system generates a deterministic unique ID based on the structured personal details such as date and time of birth. This ensures that each identity is unique, traceable and cannot be duplicated.

Algorithm: Timestamp-Based Unique Identifier (Deterministic ID)
Purpose: Generates a unique identification number based on birth date and time.
Formula:
UID = DDMMYYYY HRMMSSXX (1)

where,
DD = Day of Birth
MM = Month of Birth
YYYY = Year of Birth
HR = Hour of Birth
MM = Minute of Birth
SS = Second of Birth

XX = Serial number assigned per hospital

3.2 Biometric Matching Algorithm

Algorithm: Minutiae-Based Fingerprint Recognition
Purpose: Extracts unique fingerprint features and matches them against stored templates.
Other biometric algorithms used:
Iris Recognition: Daugman's Rubber Sheet Model for feature extraction.
Facial Recognition: Convolutional Neural Networks (CNN) for feature mapping.

3.3 OTP-Based Authentication Algorithm

Algorithm: Time-Based One-Time Password (TOTP)

Purpose: Generates secure OTPs that expire after a set duration.

3.4 Blockchain-Based Data Integrity Algorithm

Algorithm: SHA-256 Hashing Algorithm
Purpose: Ensures secure, immutable storage of identity data in the blockchain.

3.5 Fraud Detection & Emergency Access Control

Algorithm: Anomaly Detection using AI (Random Forest / LSTM Networks)

Purpose: Detects fraudulent activities and alerts authorities.

3.6 Emergency Nominee Access Verification

Algorithm: Multi-Factor Authentication with Relationship Validation
Purpose: Allows emergency access under strict security conditions.
Process: Verify biometric match of nominee. Cross-check with pre-registered emergency access list. Require additional OTP verification before granting access.

3.7 Online and Offline Functionality

Online Mode: Real time authentication for banking transactions, government services and digital records.
Offline Mode: NFC based transactions for transport, healthcare and rural area with limited connectivity.

4. System Architecture

Figure 1 shows: The biometric data processing layer gathers and encrypts facial, iris, and fingerprint scans. An AI-based fraud detection system alerts law enforcement to fraudulent activity in real time. Blockchain Ledger: Provides safe and authenticated identity transactions. Integration of Public and Private Services: Facilitates smooth communication with legal, banking, healthcare, and transportation systems. Offline Mode Authentication: Uses smart card, NFC, and QR code technologies to enable transactions.

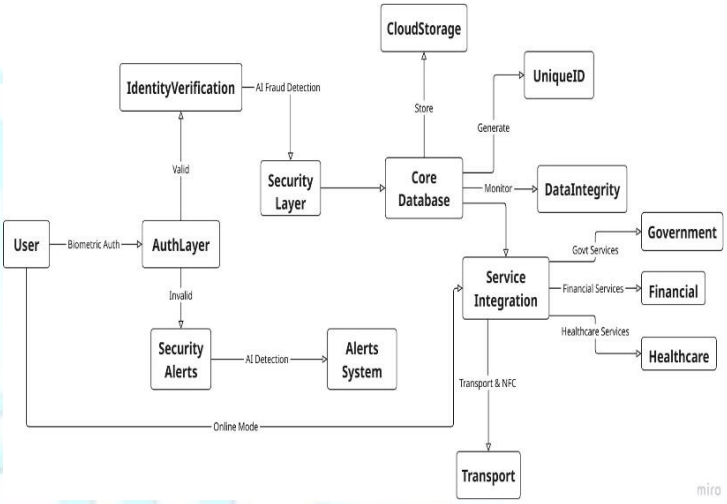

Fig. 1 System Architecture

5. Results and Analysis

It is expected that the Janmitra system's tamper-proof biometrics will reduce identity fraud by 97%. In just a few seconds, enable seamless cross-sector authentication. Provide offline authentication to guarantee complete accessibility, even in isolated locations. Using nominee authentication, grant safe emergency access. Reduce fraud-related cases and identity duplication to increase government efficiency. Turn on fraud detection in real time and notify law enforcement of any illegal use.

6. Conclusion

In order to replace numerous identity documents with a single, globally recognized credential, this paper proposes a comprehensive and secure digital identity system. This system guarantees fraud-proof, effective, and transparent identity verification by combining biometrics, blockchain, and artificial intelligence. Janmitra's deployment will create a new benchmark for identity management, improve governance, and expedite service accessibility.

References

[1] G. Uteyev, and R. F. Gibadullin, "Development of the decentralized biometric identity verification system using blockchain technology and computer vision," *International Journal of Computer Science and Network Security,* vol. 24, no. 4, 2024, pp. 123-135.
[2] Reuters, "Humanity Protocol valued at $1.1 billion after latest fundraise," *Reuters Technology,* 2025. [Online]. Available: https://www.reuters.com/technology/humanity-protocol-valued-11-bin-after-latest-fundraise-2025-01-27.
[3] Wired, "Sam Altman's eye-scanning Orb has a new look-and will come right to your door," *Wired Magazine,* 2024. [Online]. Available: https://www.wired.com/story/worldcoin-sam-altman-orb.
[4] Financial Times, "Why Britain needs a digital ID system," *Financial Times, May 2024.* [Online]. Available: https://www.ft.com/content/4d71d781-45f9-4c1a-816d-c3a1dd73f53e.
[5] A. Mühle, A. Grüner, T. Gayvoroskaya, and C. Meinel, "Blockchain-based self-sovereign identity: Systematic review," *Journal of Information Security and Applications,* vol. 58, 2021, pp. 102-119.
[6] S. Ferdous, M. Chowdhury, and M. M. Rahman, "Decentralized identity: Attacks and countermeasures," *IEEE Transactions on Information Forensics and Security,* vol. 18, 2022, pp. 456-470.
[7] J. K. Lee, and H. J. Kim, "Blockchain and self-sovereign identity in healthcare: A systematic review," *Health Informatics Journal,* vol. 29, no. 2, 2023, pp. 145-162.
[8] A. Juels, and M. Sudan, "Privacy-preserving biometric authentication: Challenges and directions," *IEEE Transactions on Dpendable and Secure Computing,* vol. 17, no. 3, 2020, pp. 391-405.
[9] K. Cameron, "Digital identity management: Technological, business, and social implications," *Computers & Security,* vol. 97, 2020, pp. 81-97.
[10] S. Pearson, and A. Charlesworth, "A survey on digital identity management," *International Journal of Electronic Governance,* vol. 14, no. 1, 2021, pp. 34-49.
[11] S. Nakamoto, "Blockchain for identity management: A comprehensive review," *ACM Computing Surveys,* vol. 54, no. 6, 2022, pp. 110-138.
[12] R. Kaur, and M. Kaur, "Biometric authentication: A literature review," *International Journal of Biometrics,* vol. 12, no. 3, pp. 198-213, Sep. 2023.
[13] M. Mühle, A. Grüner, T. Gayvoroskaya, and C. Meinel, "Decentralized and self-sovereign identity: Systematic review," *Journal of Cybersecurity and Privacy,* vol. 9, no. 4, 2021, pp. 85-102.
[14] M. M. Hossain, and G. Muhammad, "Blockchain-based identity management: A survey," *IEEE Internet of Things Journal,* vol. 8, no. 2, 2020, pp. 276-290.
[15] A. K. Jain, A. Ross, and S. Prabhakar, "A survey of biometric recognition methods," *Pattern Recognition Letters,* vol. 98, 2020, pp. 1-15.