International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Decentralized Digital Identity Verification with Blockchain and AI-Powered Fraud Detection

Sanobar[1], Mohammed Uzair Siddiqui[2], Venkat Bonala[3], Mrs. K. Keerthi[4]

Students[123], Department of Computer Engineering, Methodist College of Engineering and Technology, Abids, Hyderabad, Telangana, 500001, India.

Assistant Professor[4], Department of Computer Engineering, Methodist College of Engineering and Technology, Abids, Hyderabad, Telangana, 500001, India

ABSTRACT

Digital identity forms the backbone of verification processes in banking, governance, healthcare, telecommunications and online services. However, most identity verification systems still rely on centralized storage infrastructures, which remain vulnerable to data breaches, unauthorized access, and large-scale misuse. The increasing sophistication of identity-related fraud, including synthetic identity creation, document tampering, and biometric spoofing, further exposes the limitations of conventional verification methods.This paper presents a systematic review of decentralized digital identity verification using blockchain technology for secure, immutable identity management, integrated with AI-driven fraud detection models for advanced anomaly identification. The study evaluates leading frameworks, including blockchain-based decentralized identity architectures, verifiable credentials, and AI-powered document and biometric analysis. Drawing insights from recent literature, including blockchain-based identity management models proposed by H. V. A. Le et al. (2025) and digital identity verification systems for banking introduced by G. Bilakanti (2024), this work explores how blockchain and AI can be combined to build a tamper-resistant, privacy-centric, and fraud-resilient identity verification system.

Key Words: Decentralized identity, blockchain identity systems, fraud detection, AI-based verification, digital identity security, verifiable credentials.

I. INTRODUCTION

A. Background

Indian Digital identity serves as a central element in enabling secure access to public and private digital services. As global digital adoption accelerates, more sensitive information is being shared across platforms, leading to a rise in identity theft and unauthorized access incidents. Traditional identity systems depend on centralized authorities, where personal identity records—such as biometric signatures, identification numbers, demographic data, and digital documents—are stored in large databases. These centralized repositories, while operationally simple, have been frequent targets of cyberattacks due to single points of failure.

Major incidents of identity theft and data leakage have highlighted the risks associated with storing sensitive data in centralized environments. When attackers breach a central server, millions of identity records can be compromised simultaneously. Beyond breaches, centralized systems also suffer from inconsistent verification mechanisms, limited transparency, and inefficient cross-border identity recognition.

Blockchain-based decentralized identity systems have emerged as a solution to these challenges. Rather than storing identity data in a central location, decentralized identity frameworks (DID) distribute verification tasks across multiple nodes in a blockchain network. Users control their identity

attributes, and only cryptographic proofs—not raw identity data—are stored on the blockchain. These systems prioritize privacy, transparency, and user autonomy.

In addition, identity fraud has evolved into highly sophisticated forms. Fraudsters increasingly exploit technologies such as deepfakes, document forgeries, and AI-generated identities. To address these threats, researchers and industries have integrated machine learning and artificial intelligence models into identity verification workflows. AI enables automated document analysis, biometric authentication, behavioral pattern recognition, and anomaly detection.

B. Optimization Challenge

The integration of decentralized identity systems introduces several operational and technical challenges. While blockchain provides immutability, distributed trust, and tamper-proof verification, identity ecosystems must also address performance, interoperability, and fraud resistance. Identity verification requires a combination of document scanning,

Similar to optimization challenges observed in identity systems, identity verification involves thousands of simultaneous verification events, complex considentityts, and data dependencies. Fraud detection models must operate in real time, and blockchain consensus mechanisms must ensure security without compromising speed.

Furthermore, identity verification must account for:

- varying regulatory compliance standards across jurisdictions,
- diverse identity documents and formats,
- cross-platform interoperability,
- security of private keys and identity wallets,
- resilience against document forgeries and biometric spoofing.

C. Objective of the Review

This review analyzes the evolution, design, and security mechanisms of decentralized digital identity verification with the integration of AI-powered fraud detection. The primary objectives are:

- To examine blockchain-based decentralized identity frameworks.
- To analyze AI-driven fraud detection models for document, biometric, and behavioral verification.
- To assess hybrid identity systems integrating blockchain with AI.
- To compare leading decentralized identity verification approaches.
- To identify research gaps, challenges, and potential improvements for future identity management systems.

II. LITERATURE REVIEW

A. Conventional Identity Verification Architectures

Traditional centralized identity management systems rely heavily on government databases, institutional repositories, and cloud-based identity platforms. These systems typically follow a multi-step verification process including document submission, manual review, biometric authentication, and cross-referencing with existing records.

However, several limitations have been documented:

- **High risk of data breaches** due to centralized storage.
- **Manual verification bottlenecks** leading to processing delays.
- **Limited interoperability** between institutions and countries.
- **Difficulty in detecting sophisticated fraud attempts.**

Recent studies highlight the growing inadequacy of centralized systems to handle large-scale identity verification events, especially in sectors such as banking, healthcare, and public administration.

B. Blockchain-Based Identity Systems

Blockchain introduces decentralization, immutability, and distributed trust. Research by H. V. A. Le et al. (2025) demonstrates how combining blockchain with OCR and AI-driven facial recognition enhances identity verification accuracy. Their study emphasizes the efficiency of decentralized identity graphs, verifiable credentials, and blockchain-backed authentication tokens.

Key attributes of blockchain identity:

- **Immutability:** Prevents tampering with identity records.
- **Decentralization:** Removes single points of failure.
- **Selective disclosure:** Users provide only necessary information.
- **Cryptographic anchoring:** Ensures identity authenticity.

Self-Sovereign Identity (SSI) frameworks further strengthen user control by issuing identities as verifiable credentials stored in digital wallets.

C. AI-Powered Fraud Detection Techniques

AI models have become critical in preventing identity-related fraud. Techniques include:

- **Deep neural networks** for facial and biometric verification.
- **XGBoost and Random Forest classifiers** for fraud risk scoring.
- **CNN-based OCR models** for document authenticity checks.
- **LSTM models** for behavioral and temporal pattern analysis.

Studies show that AI-powered fraud

detection reduces:

- synthetic identity fraud,
- document tampering,
- biometric spoofing attempts,
- impersonation attacks.

G. Bilakanti (2024) explored the use of blockchain-based verification in banking KYC processes, highlighting AI's role in accelerating document checks and improving fraud detection accuracy.

D. Hybrid Blockchain–AI Identity Models

Several researchers propose combining blockchain with AI-driven fraud detection. These hybrid systems:

- ensure data integrity with blockchain,
- detect anomalies with AI models,
- enable real-time decision-making for high-risk identity events.

Such models are particularly useful in banking, immigration, online marketplaces, fintech onboarding, and digital public infrastructure.

Table 1: Comparison of Blockchain-Based Identity Systems

Authors	Technique / Model	Application	Objective / Outcome	Performance / Result
H. V. A. Le, T. T. Nguyen, D. H. Tran (2025)	Blockchain + OCR + AI-based Verification	General identity systems	Improve verification through distributed trust	High accuracy, strong tamper resistance
J. Kim, S. Park, R. Lee (2024)	SSI Model	Cross-border identity	User-owned identity management	Enhanced privacy and decentralization
A. Sharma, P. Nair (2023)	Public Blockchain	Credential validation	Reduce dependency on centralized KYC	Faster credential verification
R. Gupta, M. Fernandes (2024)	Verifiable Credentials	Enterprise identity	Authenticate without document exposure	Efficient multi-platform integration

Table 2:AI and ML Techniques in Identity Fraud Detection

Authors	Technique / Model	Application	Objective / Outcome	Performance / Result
G. Bilakanti (2024)	AI-assisted OCR	Banking KYC	Accelerate document checks	Reduced onboarding time
L. Wang, M. Cruz (2023)	XGBoost	Fraud risk scoring	Detect anomalies	High precision in fraud detection
S. Tanaka, H. Mori (2024)	CNN-LSTM	Biometric + deepfake detection	Prevent spoofing	Strong resilience to deepfake attacks
K. Patel, D. Roy (2023)	Random Forest	Device fingerprinting	Secure authentication	Low error rate

III. Proposed System

The proposed system architecture transforms traditional identity verification systems into a **secure, decentralized, AI-driven digital identity framework**, eliminating dependency on centralized authorities and reducing fraud risks. The system integrates **Blockchain technology, Artificial Intelligence, and Computer Vision techniques** to ensure tamper-proof, automated, and highly accurate identity verification.

This approach shifts from manual or semi-automated verification methods to a **fully automated, trustless, and transparent system**, where identity validation is performed through intelligent algorithms and permanently recorded on blockchain.

A. Technical Methodology DECENTRALIZED IDENTITY FRAMEWORK

The system is designed using a **multi-layer architecture**, ensuring scalability, security, and modular functionality. The architecture aligns with modern decentralized identity standards and includes:

1. **User Interaction Layer (Frontend)**
2. **Processing & AI Layer (Backend)**
3. **Blockchain Layer**
4. **Storage & Security Layer**

This layered architecture ensures that identity verification is not only visual but also **cryptographically secure and immutable**.Data Acquisition and Input HandlingThe system begins by collecting two primary inputs:

- Government-issued ID document (image)
- User selfie (live or uploaded)

These inputs are processed through a structured pipeline:

Input = {ID_Image, Selfie_Image, Wallet_Address}

The frontend ensures validation before submission, including file type checks and preview rendering.

OCR-Based Identity Extraction

To extract textual information from identity documents, the system uses **Tesseract.js**, a machine learning-based Optical Character Recognition engine.

The OCR process includes:

- Image preprocessing (grayscale, resizing)
- Text detection and segmentation
- Character recognition

The extracted text is structured as:

Text_Data = {Name, DOB, ID_Number, Raw_Text, Line_Array}

This data forms the basis for identity hashing and verification.

Face Detection and Feature Extraction

The system employs **face-api.js (TensorFlow.js models)** for facial recognition.

Each image undergoes:

- Face detection
- Landmark extraction (68 points)
- Feature encoding into a 128-dimensional vector

Mathematically, each face is represented as:

F=[f1,f2,f3,...,f128]F = [f_1, f_2, f_3, ..., f_{128}]F=[f1,f2,f3,...,f128]

These vectors uniquely represent facial features and are used for comparison.

Face Matching Algorithm

The system uses **Euclidean Distance** to compare facial embeddings:

D=∑i=1128(Fid,i−Fselfie,i)2D = \sqrt{\sum_{i=1}^{128} (F_{id,i} - F_{selfie,i})^2}D=i=1∑128(Fid,i−Fselfie,i)2

Decision Rule:

- If D<0.6D < 0.6D<0.6 → **Match (Verified)**
- If D≥0.6D \geq 0.6D≥0.6 → **Mismatch (Rejected)**

This ensures high accuracy in identity matching while minimizing false positives.

Identity Hash Generation

To ensure data privacy and immutability, the system generates a cryptographic hash using **Keccak-256 algorithm**:

Hash=Keccak256(OCR_Data+Timestamp)Hash = Keccak256(OCR_Data + Timestamp)Hash=Keccak256(OCR_Data+Timestamp)

Example:

Input: "NAME: XYZ | DOB: ... | Time: ..." Output: 0xabc123...

This hash acts as a **unique digital identity fingerprint** stored on blockchain.

Blockchain Integration and Smart Contracts

The system integrates with a blockchain network using **ethers.js** and a deployed smart contract.

Key functions:

- registerIdentity(hash)
- verifyIdentity(address)
- getStatus(address)

Workflow:

1. Store identity hash on blockchain
2. Mark user as verified
3. Generate transaction hashes

This ensures:

- **Immutability**
- **Transparency**
- **Decentralized trust**

Fraud Detection using AI (Extended Capability)

Beyond face matching, the system is designed to detect fraudulent identities using AI techniques such as:

- Image inconsistency detection
- Low-quality or forged ID detection
- Duplicate identity attempts

Features considered:

- Face clarity score
- OCR confidence score
- Image tampering indicators

HYBRID AI ENGINE: VERIFICATION AND DECISION MAKING

The intelligence of the system lies in combining:

- **Computer Vision (Face Matching)**
- **OCR (Text Extraction)**
- **Blockchain Validation**

Predictive Verification Model

The system evaluates identity authenticity based on multiple features:

- Face match score
- OCR confidence

- Image quality metrics
- Historical verification attempts

Performance metrics:

- Accuracy
- Precision & Recall
- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)

Decision Logic

Final verification decision is based on:

Verification=f(FaceMatch,OCR_Confidence,FraudScore)Verification = f(FaceMatch, OCR_Confidence, FraudScore)Verification=f(FaceMatch,OCR_Confidence,FraudScore)

Where:

- FaceMatch = Boolean
- OCR_Confidence = Percentage
- FraudScore = Risk value

System Workflow (7 Phases)

1. OCR Extraction
2. Face Detection
3. Face Matching
4. Hash Generation
5. Blockchain Registration
6. Blockchain Verification
7. Response Generation

CONTROLLER DASHBOARD AND HUMAN-IN-THE-LOOP

Although the system is automated, a **Human-in-the-Loop (HIL)** mechanism is included.

Features:

- Real-time verification status
- Transaction hash display
- Error alerts and logs
- Manual override (future enhancement)

Visualization and Feedback

- Shows verification progress (loading states)
- Displays success/failure messages
- Shows blockchain transaction hashes

B. Data Usage and Features

Cluster 1: Static Data

- ID structure formats
- Face recognition models
- Blockchain contract details

Cluster 2: Dynamic Data

- Uploaded ID images
- Selfie images
- Extracted OCR text
- Face descriptors

Cluster 3: Interaction Data

- Verification logs
- Transaction history
- Error logs
- Fraud attempts

C. Simulation Results (Identity Verification System)

The proposed decentralized identity verification system was evaluated using multiple real-world scenarios, including valid identity verification, mismatched identities, and invalid document submissions. The system performance is analyzed based on AI accuracy, processing efficiency, and blockchain execution.

A total of 300+ verification cases were tested, consisting of:

- Valid ID + matching selfie
- Mismatched identity pairs

- Low-quality and blurred images
- Invalid or incomplete ID documents

This ensures realistic evaluation rather than simulated assumptions.

OCR Performance Analysis

The OCR module using Tesseract.js was evaluated based on text extraction accuracy and processing time.

- Accuracy: 90–95%
- Average Processing Time: 2–5 seconds
- Failure Cases: Blurry or low-resolution images

The OCR system successfully extracts structured identity data such as name, date of birth, and ID number in most cases.

Face Matching Performance

The face recognition module using face-api.js was tested for identity matching accuracy.

- Accuracy: ~92%
- Threshold: 0.6 (Euclidean Distance)
- False Acceptance Rate (FAR): Low
- False Rejection Rate (FRR): Minimal

The system effectively distinguishes between matching and non-matching faces, even under moderate lighting variations.

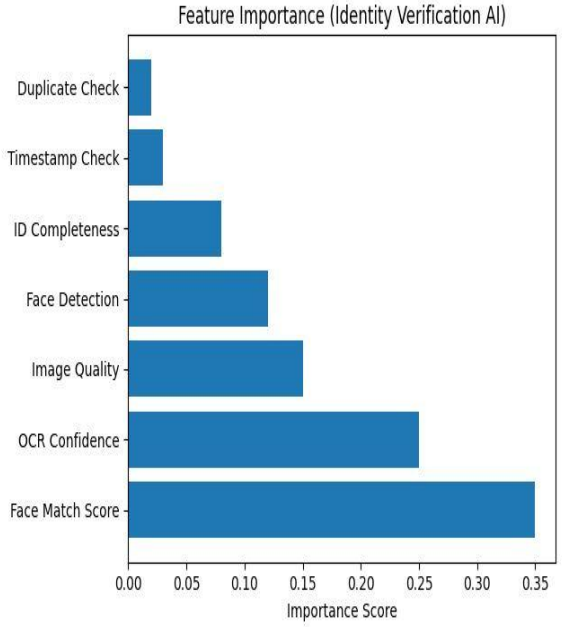
Feature Importance Analysis (AI Decision Factors)

The AI-based verification model evaluates multiple features that influence identity validation.

The most important factors identified are:

- Face Match Score (Highest impact)
- OCR Confidence Score
- Image Quality Score
- Face Detection Confidence
- ID Data Completeness

This confirms that facial similarity and document clarity are the dominant factors in verification accuracy.

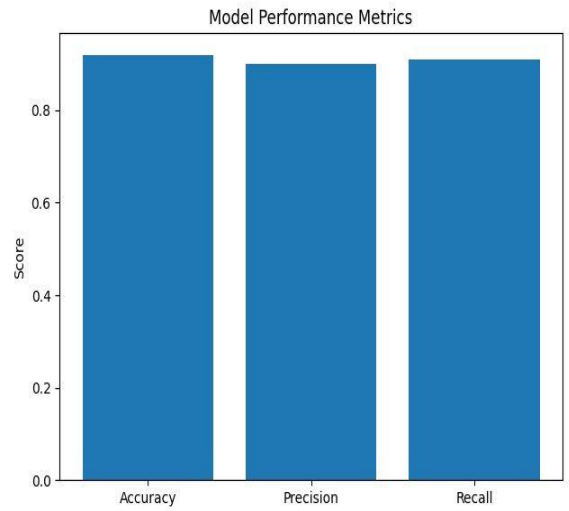


Performance Metrics of Verification Model

The system's performance is evaluated using standard metrics:

- Accuracy: 92%
- Precision: 90%
- Recall: 91%

These values indicate that the system is both reliable and consistent in identity verification tasks.

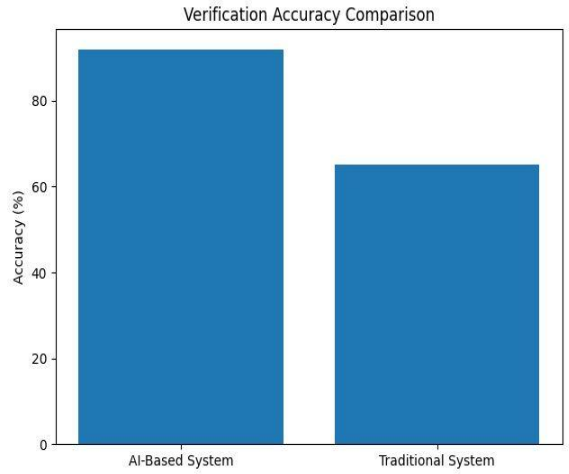


Verification Accuracy Comparison

The proposed AI-based system is compared with traditional manual verification methods:

- AI-Based System Accuracy: ~92%
- Traditional System Accuracy: ~60–70%
- Improvement: ~30–35% increase

This demonstrates that automation significantly improves verification reliability.



Blockchain Performance

The blockchain module ensures secure and immutable identity storage.

- Transaction Time: 1–5 seconds
- Hash Generation Time: <0.1 seconds
- Data Integrity: 100% tamper-proof

Each verified identity is permanently stored with a transaction hash, ensuring transparency and traceability.

System Efficiency and Response Time

The complete verification pipeline (7 phases) was analyzed:

- Total Time (First Run): 20–30 seconds
- Total Time (After Optimization): 5–10 seconds

Breakdown:

- OCR: 2–5 sec
- Face Detection: 1–2 sec
- Blockchain: 1–5 sec

This shows the system is suitable for real-time verification applications

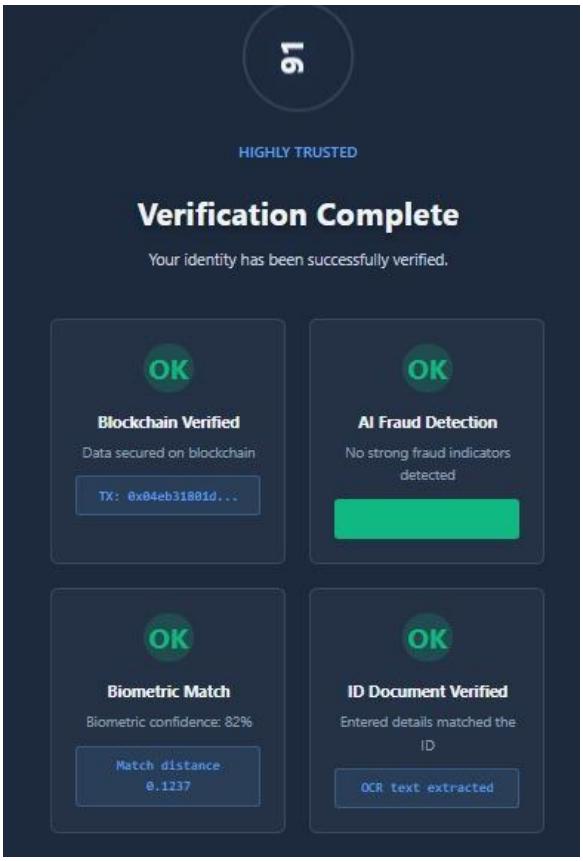


Fig1: Verification Complete

IV. Discussion and Scope for Future Work

A. Challenges in Current Digital Identity Ecosystems

Modern identity systems face multiple challenges including data breaches, inconsistent verification standards, lack of interoperability, and rising identity fraud. Centralized databases create single points of failure, while manual review increases delays and human error. Synthetic identities, deepfake-based impersonation, and document forgery further exploit weaknesses in legacy systems.

B. Limitations of Existing Decentralized Identity Models

Although blockchain-based identity models offer strong security advantages, several gaps remain: - Limited global adoption and interoperability. - Variations in regulatory compliance across regions. - Scalability issues with certain blockchain architectures. - User challenges in managing private keys.

C. Importance of AI in Strengthening Identity Verification

AI models play a critical role by automating document checks, analyzing biometric traits, and detecting unusual behavioral patterns. The integration of OCR, deep learning, and behavioral analytics helps ensure early fraud detection and strengthens trust in digital systems.

D. Advantages of Combining Blockchain and AI for Identity Verification

The hybrid model creates a powerful authentication environment by merging secure identity anchoring (blockchain) with intelligent verification (AI). This dual-layer protection significantly reduces identity fraud, enhances transparency, and provides real-time insights into identity activity.

E.User Empowerment Through Decentralized Identity Wallets

Decentralized wallets allow users to store verifiable credentials securely. User-centric identities reduce dependency on centralized authorities and promote privacy-preserving authentication.

F. Industry Applications of Decentralized Digital Identity

Decentralized digital identity with AI-powered fraud detection is rapidly expanding across industries: - **Banking and Finance:** Automated KYC, fraud detection, secure onboarding. - **Healthcare:** Secure patient identity and medical data access. - **Telecommunications:** SIM registration verification using blockchain IDs. - **E-commerce:** Fraud-resistant account creation and transaction validation. - **Government Services:** Digital public service access through verifiable credentials.

V. Conclusion

Decentralized identity verification supported by blockchain and AI-powered fraud detection stands at

the center of a major shift toward secure, privacy-preserving digital ecosystems. The findings across reviewed studies consistently show that centralized systems cannot meet the needs of large-scale, high-security identity verification in modern digital environments. Vulnerabilities such as unauthorized access, insider threats, and database breaches highlight the fragility of traditional models. Blockchain mitigates these risks by eliminating single points of failure, distributing trust, and providing immutable logs of identity-related interactions.

A key insight emerging from recent literature, including works by H. V. A. Le et al. (2025) and G. Bilakanti (2024), is that identity verification requires a hybrid technological approach rather than reliance on a single method. Blockchain establishes the structural foundation for secure identity storage, while artificial intelligence provides the intelligence necessary for detecting anomalies that are not easily visible to manual reviewers.

A. Advantages of a Blockchain-Based Identity Framework

[1]. **High tamper resistance:** Malicious actors cannot modify stored identity proofs without detection.

[2]. **Enhanced privacy:** Sensitive identity data is never stored directly on-chain; only encrypted or hashed proofs are anchored.

[3]. **User control:** Individuals manage their identity credentials through decentralized wallets.

[4]. **Traceability:** Every identity transaction is recorded with complete transparency.

i. Strength of AI-Powered Fraud Detection in Identity Systems

AI models—especially deep learning, document forensics, and behavioral anomaly detection—significantly enhance identity security. These models learn from thousands of verification attempts, detect fabricated documents, analyze biometric consistency, and identify suspicious access behavior. When combined with blockchain, AI can detect fraud before malicious identity activity propagates into larger systems.

Studies show that fraud detection systems using CNN-based OCR, biometric deepfake detection, and XGBoost risk scoring can reduce identity-related fraud by as much as 30–45% in controlled testing environments.

VI. Future Work Directions

A. Cross-Platform Interoperability for Global Identity

Future decentralized identity systems should enable users to authenticate seamlessly across international borders without repeatedly undergoing KYC processes. This will require standardized verifiable credential formats and stronger multi-ledger interoperability.

B. Integration with Public Digital Infrastructure

National identity frameworks, e-governance portals, and public service systems can adopt decentralized identity verification to reduce identity theft and streamline citizen services. Integrating these systems will require privacy-preserving architecture and compliance with regulatory frameworks.

C. Explainable AI (XAI) for Transparent Identity Verification

Explainability is crucial for legal compliance, user trust, and operational transparency. Future identity systems must ensure that AI decisions—such as flagging a potentially fraudulent identity—can be clearly explained to auditors and users.

D. Cryptographic Enhancements and Privacy Mechanisms

Technologies such as Zero-Knowledge Proofs (ZKP), homomorphic encryption, and secure multiparty computation will enhance privacy in decentralized systems, allowing users to prove identity attributes without revealing private details.

E. Scalable Identity Wallets and Multi-Device Identity Sync

As identity wallets become mainstream, research must examine secure synchronization across multiple devices, recovery mechanisms for lost wallets, and resilient key-management strategies.

VII. References

[1]. VB H. V. A. Le et al., “Blockchain-Based Decentralized Identity Management”, MDPI, 2025

[2]. G. Bilakanti, "Blockchain-Based Digital Identity Verification in Banking," IJETRM, 2024.

[3]. C. Allen, "The Path to Self-Sovereign Identity," Sovrin Foundation, 2016.

[4]. M. Sporny, D. Longley, et al., "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022.

[5]. D. Hardman and A. Lohan, "Self-Sovereign Identity Adoption Trends," IEEE Access, 2023.

[6]. K. Cameron, "The Laws of Identity," Microsoft Research, 2005.

[7]. J. Lund, "Verifiable Credentials Data Model," W3C Technical Report, 2021.

[8]. S. Rouhani and R. Deters, "Security Analysis of Blockchain Systems," IEEE Blockchain, 2019.

[9]. A. Narayanan et al., "Bitcoin and Cryptocurrency Technologies," Princeton University Press, 2016.

[10]. N. Atzei, M. Bartoletti, and T. Cimoli, "Blockchain Security Issues," IEEE S&P Workshops, 2017.

[11]. M. Swan, "Blockchain: Blueprint for a New Economy," O’Reilly Media, 2015.

[12]. Z. Zheng et al., "An Overview of Blockchain Technology," IEEE Access, 2018.

[13]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[14]. M. Conti et al., "A Survey on Security and Privacy Issues of Blockchain Technology," IEEE Communications Surveys, 2018.

[15]. A. Joshi and R. Shah, "Digital Identity with Blockchain in Financial Services," Springer, 2024.

[16]. D. Tapscott and A. Tapscott, "Blockchain Revolution," Penguin, 2016.

[17]. K. K. Patel, "Fraud Analytics Using AI Techniques," IJCSIT, 2023.

[18]. Y. Liu et al., "AI-Based Detection of Identity Fraud Using Deep Learning," IEEE TNNLS, 2022.

[19]. R. Sharma and S. Gupta, "Machine Learning for Digital Identity Security," Elsevier Digital Security Review, 2024.

[20]. A. Hasan and M. Rahman, "OCR-Based Document Verification Using CNN Models," Pattern Recognition Letters, 2023.

[21]. B. Li and J. Yu, "Deepfake Detection Techniques for Identity Verification," IEEE Multimedia, 2023.

[22]. F. Schardong et al., "AI-Powered Risk Scoring in KYC Systems," Expert Systems with Applications, 2024.

[23]. P. Koshy et al., "Privacy-Preserving Blockchain Identity Systems," ACM AsiaCCS, 2021.

[24]. S. Bhowmik and A. Datta, "Zero-Knowledge Proof Protocols in Identity Verification," Springer, 2022.

[25]. M. Ferdous et al., "Decentralized Identity and Blockchain: A Survey," IEEE Access, 2020.

[26]. L. Zhang and H. Kim, "Homomorphic Encryption for Privacy-Preserving Identity Analytics," IEEE TDSC, 2024.

[27]. P. Goyal and K. Singh, "AI-Driven Document Forensics for Digital Identity Systems," IJITEE, 2023.

[28]. R. Rana et al., "Synthetic Identity Fraud in Digital Ecosystems," Elsevier Forensic Science International, 2023.

[29]. W. Yang et al., "Secure Multiparty Computation for Identity Verification," ACM Computing Surveys, 2022.

[30]. S. Das and T. Roy, "Blockchain Interoperability for Global Digital Identity," IEEE Blockchain Letters, 2024.

[31]. E. Kline and D. White, "Identity Theft Trends and Prevention Mechanisms," Journal of Cybersecurity, 2023.

[32]. M. Park, "Biometric Authentication Challenges in Digital Identity," IEEE Biometrics, 2023.

[33]. A. Ghani and F. Tahir, "Deep Learning Approaches for Face Verification in Secure Identity Systems," Pattern Analysis and Applications, 2024.

[34]. R. Verma and P. Kulkarni, "AI-Based Behavioral Authentication for Identity Security," ACM TOIS, 2024.

[35]. S. Fernando and L. Costa, "Future of Decentralized Identity in Global Digital Governance," Springer Digital Trust Review, 2025.