International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Blockchain Based AI Identity Verification System in KBPCOES

Project Guide: **Miss Shabina Modi**
(Karmaveer Bhaurao Patil College of Engineering, Satara)
(Depatment of Computer Science and Enineering)

ABSTRACT

The review analyzes the existing literature at the convergence of blockchain technology, biometrics/AI, and digital identity verification. We gather and examine more than ten recent articles (2020–2025) that suggest frameworks, protocols, and assessments of legal/usability for blockchain-based biometric identity and self-sovereign identity (SSI) systems. We identify common design patterns—such as on-chain hashes paired with off-chain biometric templates, verifiable credentials (VCs) and decentralized identifiers (DIDs), along with smart contracts coordinating verification—uncover technical and legal challenges (like scalability, privacy-preserving biometric matching, GDPR/consent issues, and interoperability), and introduce a specific research problem: a privacy-preserving, verifiable face-liveness identity proofing framework for online examinations utilizing DIDs/VCs, homomorphic/fuzzy cryptography, and a hybrid layer-2 storage solution. We outline the proposed solution, experimental methodology, evaluation metrics, and anticipated assessment outcomes. The survey includes a table of literature, synthesis of themes, a stepwise approach to problem identification, and a suggested assortment of figures/tables for clear presentation. This paper seeks to support research initiatives and practical applications of blockchain-enabled AI identity verification.

Keywords: Blockchain, biometric authentication, self-sovereign identity (SSI), decentralized identifiers (DID), verifiable credentials (VC), face liveness, privacy-preserving biometrics, online exam proctoring.

INTRODUCTION

Digital identity verification plays a crucial role in finance, e-governance, online education (such as exams), e-voting, and access management. Centralized identity repositories are vulnerable to security breaches and privacy infringements; the integration of biometrics (unique identification through AI) and blockchain technology offers tamper-proof audit trails, user autonomy (self-sovereign identity), and automated verification through smart contracts. Major applications include: (1) Secure online exam supervision and identity verification to prevent cheating; (2) e-voting that ensures voter privacy and verification; (3) onboarding for financial services (KYC) aimed at reducing fraud; (4) transferable credentials across different domains (like academic diplomas). Challenges consist of biometric privacy concerns, scalability issues, adherence to regulations, and ensuring secure proof of liveness.

METHODOLOGY

The proposed Blockchain Backed AI Identity Verification System integrates two advanced technologies — Artificial Intelligence (AI) for identity verification and Blockchain for secure, tamper-proof storage — to build a robust, decentralized identity management framework. The methodology involves a step-by-step process starting from user registration to blockchain-based verification and access control. The system architecture consists of four main modules: User Registration, AI Verification, Blockchain Storage, and Secure Access Control. Each module works collaboratively to ensure a seamless and highly secure identity verification process.

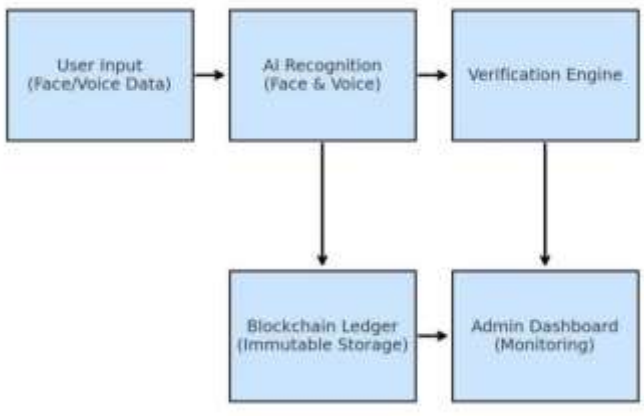

Fig1: System Diagram

The system is designed using a modular approach. The main modules include:

1. User Registration Collection of user information and documents.

2. AI Verification – Implementation of AI-based algorithms for face and document matching.

3. Blockchain Storage – Storing verified identities in an immutable ledger.

4. Access Control – Controlled data retrieval using cryptographic keys

BACKGROUND

Blockchain fundamentals: decentralized and unchangeable ledgers, consensus mechanisms, and smart contracts (for automation). In public blockchains, the trade-off lies between immutability and transparency versus privacy and expenses; permissioned blockchains (such as Hyperledger Indy/Aries) cater to identity-related applications.Self-Sovereign Identity (SSI), DIDs & VCs: SSI empowers individuals with control over their credentials; Decentralized Identifiers (DIDs)

serve to identify subjects, while Verifiable Credentials (VCs) provide signed attestations that can be validated without the need for centralized databases. Numerous SSI frameworks (including Sovrin, Indy, and Jolocom) are pertinent.

Biometrics and AI fundamentals: Biometric systems (face, fingerprint, iris recognition) involve enrollment (template creation) and matching processes (1:1 or 1:N). Contemporary facial recognition employs deep neural networks (embedding and metric techniques). Liveness detection serves to prevent spoofing attempts. Biometric templates are sensitive in nature; therefore, storage practices should not involve raw templates on-chain.

LITERATURE REVIEW

#	Citation (short)	Year	Contribution / Method	Key result / Note
1	Zaeem et al., Blockchain-based SSI (ACM)	2021	Comprehensive SSI survey; frameworks & principles	SSI frameworks compared; adoption challenges. (ACM Digital Library)
2	ArXiv: Blockchain & Biometrics (survey + GDPR)	2023	Survey combining legal analysis (GDPR) with tech options	Highlights privacy tradeoffs and need for off-chain solutions. (arXiv)
3	Salem et al., Blockchain-based biometric identity mgmt (Springer)	2024	Architecture for face recognition + blockchain; hash on-chain	Proposes enrollment/auth phases; recommends off-chain templates. (SpringerLink)
4	IET Review: Blockchain deployment for biometric systems	2024	Survey on coupling blockchain + biometrics	Reviews storage options and threat models. (IET Research)
5	Alzahab et al., Decentralized biometric auth (fuzzy)	2025	Fuzzy commitments + smart contracts for matching	Demonstrates feasibility of fuzzy crypto in decentralised setting. (ScienceDirect)

6	MDPI: Decentralized Identity Mgmt	2025	System design using Merkle trees, OCR & blockchain	Shows hybrid on/off-chain verification scheme. (MDPI)
7	Frontiers: SSI contextualization & frameworks	2024	Comparative analysis of SSI projects (Sovrin, KILT, Litentry)	Useful for platform selection and compliance mapping. (Frontiers)
8	ScienceDirect: Online exam framework w/ blockchain	2023	End-to-end blockchain framework for online exams	Demonstrates integrity and auditability for submitted results. (ScienceDirect)
9	Nature Sci Rep: Exam cheating detection & blockchain	2025	Survey + empirical results on exam integrity tools	Emphasizes multi-modal verification (biometric + behavior). (Nature)
10	ResearchGate: BBAS — Blockchain-based Biometric Auth System	2025	Proposes hybrid storage + smart-contract policy	Discusses encryption and hashed proofs on-chain. (ResearchGate)
11	arXiv: DIDs & Verifiable Credentials survey	2025	Technical overview of DIDs/VCs and threats	Good source for standards and interoperable flows. (arXiv
12	Various 2023–25 reviews (ScienceDirect / SRJ)	2023–2025	Multiple surveys on decentralized identity & authentication	Converging recommendations: keep raw biometrics off-chain, use cryptographic bindings. (sirjana.in)

Cross-paper synthesis

- Hybrid architecture involves storing biometric templates in secure off-chain locations (such as secure storage or encrypted IPFS) while keeping hashes or commitments on-chain to ensure integrity and facilitate auditing.
- The adoption of SSI and VCs entails utilizing DIDs/VCs to hold identity attestations, with blockchain primarily serving as trust anchors and for managing revocation registries.
- Privacy-preserving biometric techniques like fuzzy commitments, secure multiparty computation (MPC), and homomorphic encryption have been suggested but are seldom comprehensively assessed on a large scale.
- Deployment in specific domains, such as online examinations and electronic voting, has resulted in tangible prototypes; however, thorough evaluations concerning usability and legal compliance are sparse.

RESEARCH GAPS

- **Scalability and the expenses associated with on-chain operations** — there are few studies that assess transaction throughput and costs in realistic high-demand situations (for example, large-scale online exam events).
- **Practical methods for privacy-preserving biometric matching** — although there is discussion regarding fuzzy cryptography and secure enclaves, there is a scarcity of comprehensive evaluations that integrate liveness detection, privacy, and accuracy in the face of adversarial spoofing attempts.
- **Interoperability among self-sovereign identity (SSI)** frameworks — while various frameworks are available, there is a lack of comparative studies showcasing real-world deployments of decentralized identifiers (DIDs) and verifiable credentials (VCs) interoperability.
- **Legal and compliance research at the deployment level** — there are few empirical investigations concerning GDPR and consent in blockchain-based biometric systems, particularly when immutable ledgers challenge the "right to be forgotten."
- **Usability and accessibility** — there is limited user-focused assessment regarding user experience (UX), enrollment efforts, and error rates across different demographics.

SYSTEM ARCHITECTURE

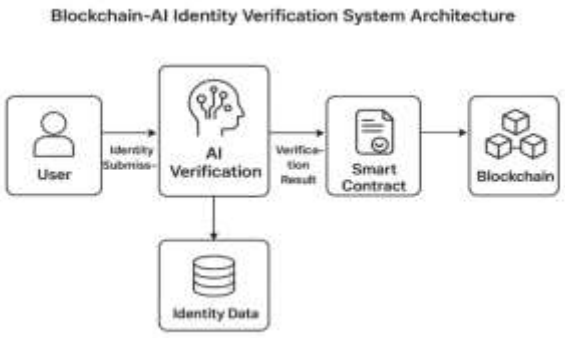

Fig 2: System Architecture

1. User

- Function: The entry point of the system.
- The user provides identity information this may consist of:
- Biometric information (facial recognition, fingerprint, iris scan)
- Identification documents (Aadhar, passport, university identification)
- Metadata (timestamp, geographic location, device identification)

Purpose:

Initiates the identity verification procedure while ensuring secure data transmission to the AI module.

2. AI Verification

- Core Role: Employs AI and machine learning techniques for biometric identification and validation.
- Example: Advanced deep learning algorithms for facial recognition or liveness testing.
- Confirms authenticity (identifies spoofing or deepfake attempts).

Processes:

- Data preprocessing → feature extraction → matching → result determination.

Storage Integration:

- Simultaneously saves encrypted biometric features or identity embeddings in the Identity Data module.

3. Identity Data

- Purpose: Securely holds identity-related information.
- This information is:

  Encrypted.

- Can be archived off-chain (to ensure privacy) while its hash is recorded on-chain to preserve immutability.
- Benefit: Safeguards sensitive biometric information from unauthorized access and alteration.

4. Smart Contract

- Role: Manages the automation of verification and access rights.
- Following the AI verification stage:

- The verification outcome is communicated to a smart contract.

The contract establishes stipulations such as:

- Who has permission to access the identity data.
- When the verification is considered valid.

5. Blockchain

- Core Function: Serves as a secure ledger for all identity-related transactions and verification records.
- Stores identity verification proofs and their hashes (not the raw data).
- Offers transparency, decentralization, and traceability.

Benefits:

- Prevents identity fraud and duplicate identities.

Algorithm:
Step 1- Capture Identity Input
Step2- Hashing & Pre-Storage Security **Step3-** AI-Based Identity Verification **Step4-** Fraud Evaluation & Decisioning
Step5- Build Verifiable Credential Creation (If Approved)
Step6- Blockchain Anchoring
Step7- Store Audit Report (Off-Chain) **Step8-** Return Result

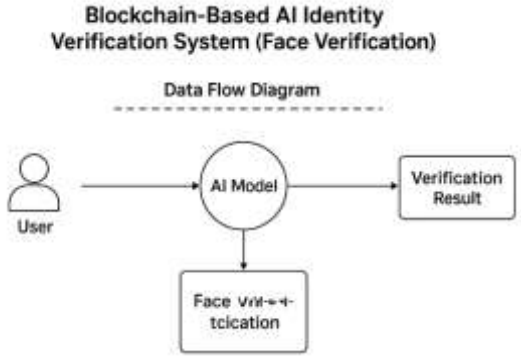

Fig3: Flow Diagram

FUTURE SCOPE

Privacy-Safeguarding Biometric Verification:

- Innovate sophisticated homomorphic encryption and secure multi-party computation (MPC) methodologies that enable biometric verification without disclosing the raw template.
- Investigate zero-knowledge proofs (ZKPs) for confirming identity assertions without sharing sensitive information.

Standardization of SSI Frameworks:

- Establish interoperable formats for DIDs (Decentralized Identifiers) and Verifiable Credentials (VCs) across various blockchain networks.
- Create standardized APIs and open protocols to facilitate seamless identity verification across different platforms.

CONCLUSION

The combination of blockchain technology and AI-based biometric systems presents a revolutionary approach for secure and transparent verification of digital identities. In contrast to conventional centralized systems, where third parties manage user information, blockchain guarantees decentralized trust, tamper-proof audit trails, and ownership of data. When integrated with AI-driven biometric identification methods, such as facial recognition or fingerprint scanning, this technology enhances authentication by linking identities to distinct biological characteristics, thereby reducing the risk of impersonation and fraud.In areas like online testing, e-voting, and digital onboarding, this integration ensures that only authorized individuals can engage, with every verification being recorded on a distributed ledger. Nevertheless, the survey indicates a number of ongoing challenges:A shortage of scalable privacy-preserving algorithms for matching biometric data.Thus, while the amalgamation of blockchain and AI for identity verification shows considerable potential, it necessitates further research and frameworks for practical implementation to foster global trust and acceptance.

REFERENCES

1. R. Nokhbeh Zaeem, et al., "Blockchain-Based Self-Sovereign Identity: Survey and Open Research Challenges," *ACM Computing Surveys*, 2021. ACM Digital Library
2. A. Gomez-Barrero, et al., "Blockchain and Biometrics: Survey, GDPR Analysis, and Research Challenges," *arXiv preprint*, 2023. arXiv
3. S. H. G. Salem, et al., "Blockchain-based biometric identity management," *Cluster Computing* / Springer, 2024. SpringerLink
4. N. Alzahab, et al., "Decentralized biometric authentication based on fuzzy commitments," *ScienceDirect*, 2024. ScienceDirect
5. HVA Le, et al., "Blockchain-Based Decentralized Identity Management" (MDPI), 2025. MDPI
6. R. A. Pava-Díaz, et al., "Self-sovereign identity on the blockchain: contextualization and frameworks," *Frontiers in Blockchain*, 2024. Frontiers
7. M. R. I. Sattar, "An advanced and secure framework for conducting online exams using blockchain," *ScienceDirect*, 2023. ScienceDirect
8. H. Wang, et al., "Online exam cheating detection and blockchain trusted framework," *Nature Scientific Reports*, 2025. Nature
9. "Blockchain-based Biometric Authentication System (BBAS)", ResearchGate preprint, 2025. ResearchGate
10. J. Xian, "A survey on decentralized identity management systems," *ScienceDirect*, 2025. ScienceDirect
11. "A survey on decentralized identifiers and verifiable credentials," *arXiv*, 2025. arXiv
12. Additional surveys and whitepapers: SRJ (2024), IJISRT survey pages (2023–2025).