Decentralized Digital Identity: A Blockchain and Neural Network Approach

Arvind Babu, Kozhikode Raghunathan Balasubramanian, Anisha Singh, Meenakshi Reena Sureshbabu and Yuvaraj Natarajan

ABSTRACT

Current digital identity systems face significant challenges in privacy, security, user control, and performance. This research proposes a novel blockchain-powered approach that integrates neural network technologies to address fundamental limitations of centralized identity management. By leveraging decentralized architecture and biometric authentication, we present a transformative solution to digital identity verification that enhances user privacy, security, and autonomy while mitigating systemic risks in both centralized and decentralized frameworks. Empirical evaluation demonstrates authentication accuracy of up to 97.20% and average login latency of 1.069 seconds, validating the system's effectiveness and responsiveness on standard consumer hardware.

Keywords: Neural-network FaceNet512 authentication, Proof-of-authority consensus, Hybrid IPFS-blockchain storage, Self-sovereign identity architecture, Guardian-assisted identity recovery

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Correspondence to:
Arvind Babu,
arvind.babu2022@vitstudent.ac.in

Additional material is published online only. To view please visit the journal online.

Cite this as: Babu A, Balasubramanian KR, Singh A, Meenakshi RS and Natarajan Y. Decentralized Digital Identity: A Blockchain and Neural Network Approach. Premier Journal of Science 2025;15:100142

DOI: https://doi.org/10.70389/PJS.100142

Peer Review

Received: 14 August 2025

Last revised: 26 September 2025

Accepted: 1 October 2025

Version accepted: 3

Published: 28 October 2025

Ethical approval: N/a

Consent: N/a

Funding: No industry funding

Conflicts of interest: N/a

Author contribution: Arvind Babu, Kozhikode Raghunathan Balasubramanian, Anisha Singh, Meenakshi Reena Sureshbabu and Yuvaraj Natarajan – Conceptualization, Writing – original draft, review and editing

Guarantor: Arvind Babu

Provenance and peer-review: Unsolicited and externally peer-reviewed

Data availability statement: N/a

Introduction

Digital identity systems are technological frameworks that enable individuals to authenticate and verify their identity in digital environments. These systems have become increasingly critical in our interconnected world, serving as the foundation for accessing services, conducting transactions, and maintaining personal security across online platforms.[1]

The exponential growth of digital interactions has exposed critical vulnerabilities in traditional identity management systems. Centralized digital identity frameworks are increasingly compromised by structural weaknesses that fundamentally undermine user privacy and data security.[2] These centralized systems suffer from being single points of failure, as their databases are vulnerable to comprehensive data breaches. Users have minimal autonomy over their personal information and must rely on third-party dependencies to protect and manage their sensitive data. The lack of transparency in data access mechanisms and potential misuse, combined with high security risks from concentrated data storage, make these systems attractive targets for cybercriminals.[3,4]

Decentralized identity verification represents a paradigm shift that addresses these fundamental limitations by distributing control back to individual users, eliminating single points of vulnerability, providing transparent and immutable identity management, enhancing privacy through cryptographic techniques, and enabling user-controlled data sharing.

While several Self-Sovereign Identity (SSI) frameworks such as Hyperledger Indy/Sovrin and uPort have advanced decentralized identity management,[5,6] our proposed architecture introduces specific technical modifications to address existing limitations. In contrast to Sovrin's permissioned blockchain and uPort's reliance on Ethereum, our system incorporates neural network-based biometric verification. This integration enables identity verification methods that extend beyond conventional cryptographic techniques used in current SSI implementations.[7,8] Additionally, our design adopts a hybrid storage strategy combining blockchain with the InterPlanetary File System (IPFS),[9] supporting scalability while preserving data integrity. Collectively, these architectural components form a decentralized identity solution that aims to mitigate the systemic weaknesses observed in both centralized and first-generation decentralized systems.[10]

Related Works

Standards and Established Frameworks

The W3C Decentralized Identifiers (DIDs) specification provides a framework for decentralized identity management which enables verifiable and self-sovereign digital identities. These are also complemented with Verifiable Credentials (VCs) that provide cryptographically secure digital credentials.[11] However, these rely primarily on cryptographic proofs and digital signatures while lacking integrated biometric mechanisms.

Recent years have seen the launch of large-scale SSI pilots such as the European Blockchain Services Infrastructure (EBSI),[12] a European Union initiative piloting verifiable credentials and decentralized identifiers across multiple member states. EBSI demonstrates credential interoperability and regulatory compliance at a cross-border scale, actively involving universities, service providers, and government agencies. Similarly, the IDunion[13] consortium in Germany establishes an open, federated SSI network focusing on privacy-preserving mechanisms and real-world deployment. Both initiatives illustrate the maturity and challenges of SSI in practical, regulated environments, providing valuable benchmarks for this work

Hyperledger Indy provides a permissioned blockchain designed for identity management and Aries offers protocol implementations for credential exchange.[14] These frameworks provide credential verification flows but lack native biometric integration and often require external authentication systems.

Microsoft ION (Identity Overlay Network) implements DIDs on top of Bitcoin's blockchain and also involves IPFS for off-chain storage.[5] However, it relies on the energy-intensive Proof of Work consensus that Bitcoin uses and also does not explore biometric authentication or other consensus mechanisms like Proof of Authority.[15]

In contrast, permissioned blockchains have experimented with alternative consensus protocols. Istanbul Byzantine Fault Tolerance (IBFT)[16] and Tendermint[17] are two mechanisms designed to deliver strong consistency and rapid transaction finality in trusted consortium contexts. IBFT has been adopted in enterprise-ledgers (e.g., Quorum), combining crash and Byzantine fault tolerance with performance improvements. Tendermint, widely used in inter-chain credential solutions, supports BFT guarantees and instant finality, further strengthening the scalability and fault tolerance of decentralized identity systems.

Biometric-Blockchain Integration Systems

Recent approaches explore the combination of biometrics with blockchain architecture. Yasumura et al.[7] proposed Bio-SSI for example, that uses biometric cryptosystems specifically including fuzzy extractors, which use simpler matching algorithms in comparison to deep learning models such as FaceNet512. Moreover, Bio-SSI stores encrypted VCs and helper data on public or private clouds which do not have decentralized audit logs and transparency guarantees of a hybrid IPFS -blockchain storage.

Another notable implementation is the Deep Feed-Forward Neural Network-Based Biometric Authentication System (DFNN) utilizing a biometric fingerprint image.[8] The usage of fingerprints may not be as user-friendly as facial recognition which is highly portable to modern devices (laptops, phones) equipped with cameras. Moreover, the DFNN biometric system does not explore hybrid blockchain IPFS storage and its benefits in comparison to a traditional database.[10]

Outside of conventional fuzzy extractors or cryptosystems, latest developments include:

- Cancelable Biometrics, irreversibly converting templates with matching performance maintained and allowing simple revocation or re-issuance, essential for GDPR compliance.
- Homomorphic Encryption, enabling biometric matching on encrypted data, facilitating privacy-preserving verification on cloud or distributed environments.
- Zero-Knowledge Proofs, which allow users to demonstrate ownership of a biometric feature without divulging raw information. These have been incorporated into blockchain-based authentication, and they enable robust auditability and unlinkability.

Collectively, these strategies address fundamental regulatory and technical needs, irreversibility, unlinkability, and auditability, that are necessary for implementing contemporary, privacy-focused identity frameworks at scale.[18,19]

Background and Theoretical Framework

Evolution of Digital Identity Management

Traditional digital identity systems have evolved from basic authentication mechanisms to sophisticated multi-factor verification processes. However, the predominant centralized approach continues to present significant vulnerabilities affecting both individual privacy and systematic security. These centralized systems remain susceptible to data breaches, unauthorized access, and identity theft, while offering users minimal control over their personal information.[5] Centralized databases storing sensitive personal information have become attractive targets for cybercriminals, leading to frequent and devastating data breaches.[10]

Blockchain Technology and Identity Management

Blockchain technology has emerged as a transformative advancement in digital record-keeping, providing a decentralized, cryptographically secured digital ledger that records transactions across a distributed network.[4] Its fundamental characteristics of immutability, transparency, and resistance to unauthorized modifications make it particularly suitable for identity management applications. The development of Decentralized Identifiers (DIDs) and Self-Sovereign Identity (SSI) frameworks has strengthened blockchain-based identity management systems, enabling individuals to maintain complete control over their digital identities while ensuring interoperability across different platforms and services.[8,9]

Neural Network for Biometric Authentication

The integration of neural networks with blockchain technology represents a significant advancement in biometric authentication systems. Convolutional Neural Networks (CNNs) have proven particularly effective in processing and extracting features from images like in medical imaging fields as well as facial features for authentication purposes.[8,20] The system employs these neural networks to process biometric data and extract unique feature vectors, which are then encrypted and stored securely off-chain using the InterPlanetary File System (IPFS).

Recent advancements in federated learning have enabled decentralized training of machine learning models on data across multiple devices, ensuring that sensitive data remains on the user's device, significantly reducing privacy risks. This approach leverages hybrid CNN-RNN architectures to capture spatial and temporal features of user behavior, achieving high accuracy while maintaining privacy compliance.[21,22]

Privacy-Preserving Biometric Matching

Fully Homomorphic Encryption (FHE) has emerged as a promising solution for privacy-preserving biometric matching. Recent implementations, such as Adaptive Multi-Biometric Fusion with FHE (AMB-FHE), reduce ciphertext size significantly while maintaining high security standards.[23] These protocols enable encrypted biometric templates to be matched without exposing sensitive data, ensuring compliance with modern privacy regulations, and hence, have scope in the implementation of our system.

DOI: https://doi.org/10.70389/PJS.100142 | Premier Journal of Science 2025;15:100142

Zero-Knowledge Proof-Based Identity Verification

Zero-Knowledge Proofs (ZKPs) are revolutionizing decentralized identity systems by enabling verification of claims without revealing underlying data. For example, users can prove they meet specific criteria, such as age or citizenship, without disclosing personal details like names or passport number.[24]

Motivation and Objective

The exponential growth of digital interactions demands a robust, secure, and user-centric identity management approach. Current centralized systems are increasingly inadequate in protecting individual privacy and ensuring data security.[4] Critical issues with existing solutions include massive data breaches compromising millions of user records such as the Equifax data breach of 2017,[25] unauthorized data sharing by third parties accessing and monetizing personal information, limited user autonomy with minimal control over personal digital identities, and high operational costs from inefficient centralized verification processes.[4]

The integration of blockchain's decentralized architecture with pattern recognition through neural networks creates a secure identity verification mechanism that ensures data security, provides accurate authentication and reduces fraud potential. Our key research objectives include designing a fully decentralized identity management system, implementing neural network-based biometric authentication, developing a privacy-preserving verification mechanism, creating a scalable interoperable identity framework, and demonstrating a practical alternative to centralized identity systems.

Methods

Decentralizing digital identity involves taking away all centralized storage of private identifiers, documents, biometric data and other sensitive information. All access logs to anyone's digital identity must also be public, transparent and receive appropriate permissions first. A key factor is for users to maintain control over their data and who has access to it, ensuring that their personal information is not distributed without consent.[5] Security mechanisms to protect against malicious actors are implemented through cryptographic hashes and current standard encryption methods. This is primarily for the content identifiers of biometric data stored in the IPFS for authentication but can also apply to other sensitive data if and when added.

Using the proposed digital identity, a user can theoretically authenticate himself at any KYC (know your customer) requirement, login or registration. The trust of each digital identity entirely falls on the validators of the Blockchain, which will be verified organizations or government agencies using a Proof of Authority (PoA) consensus mechanism.

Authentication is done through biometric scans like face recognition or fingerprint scans which is the so-called "key" to their digital identity. In the proposal, this biometric data in combination with Public Key Infrastructure (PKI) should suffice for linking the real person with their digital identity.[26] The overall architecture combines all the security, privacy, decentralization and authentication components to implement the project.

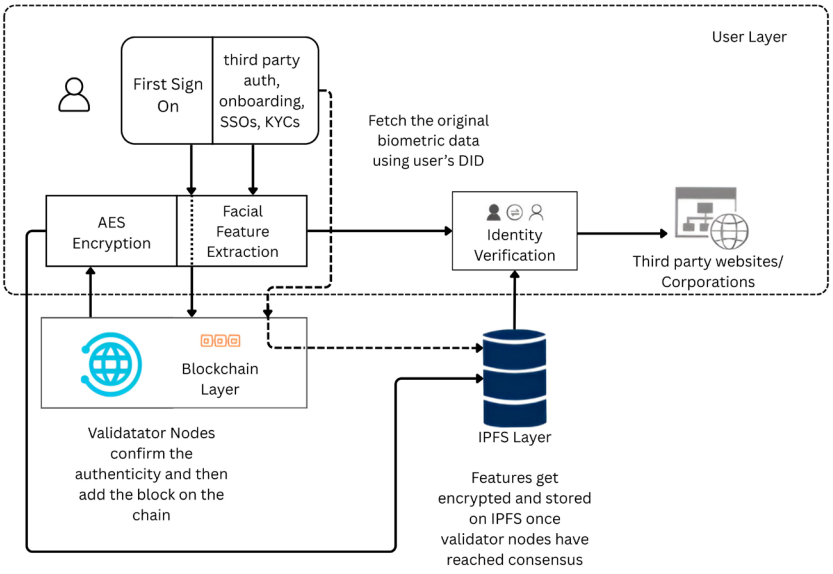

Fig 1 | System architecture

System Architecture

Figure 1 illustrates several components and roles of the architecture as explained further below.

1. Stakeholders
   - *Users:* These are the end user systems who use the system either for authentication (login/signup) or sensitive data management.
   - *Enterprises:* These are corporations or websites that rely on the system for user onboarding, authentication, SSO (single sign on) or KYC (know your customer) through verification of government records.[25]
   - *Trusted validator nodes:* Set of trusted validators that validate the transactions in PoA. Validators can include government agencies, banks or institutions
2. User Layer
   It is the entry point for identity authentication and users directly interact with the layer to register or sign in. It consists of:
   - *Biometric collection:* Captures fingerprint, facial, iris, or other biometric features from the user. This is done during the first registration on the system as well as subsequent sign-in processes by other third party websites/corporations for on-boarding, SSOs, or KYCs.
   - *Pre-processing and feature extraction:* This process converts the biometric information into feature vectors by applying pre-processing algorithms like de-noising or edge detection. The pre-processed information is then fed into neural networks which extract the feature vectors of interest.

- *User interface and authentication mechanism:* There are two UIs: one is embedded directly into third party websites for users to safely log in and the other is a dashboard to manage identity accesses and control sensitive document access.
- *Encryption and secure transmission:* Ensures Biometric data is safely encrypted before being stored in the IPFS Layer.
- *Consent and identity linking:* This links the biometric information with an identity record, guaranteeing user consent as well as adherence to privacy standards.
- *Onboarding and first sign-in:* Users will first register into our system in order to access its features. During this first registration, they will have to validate their identity with trusted nodes using a government-issued identity document.

3. Blockchain Layer:
The Blockchain layer serves as a foundation for providing decentralization, security, transparency and immutability—all of which are crucial for an identity management system. It uses Smart Contracts to automate identity verification, authentication, and access control processes, ensuring compliance and reducing human error.

The system uses PoA consensus mechanism, where trusted validators confirm transactions. This ensures energy-efficient and rapid consensus without compromising security.[27] All transactions are recorded on the blockchain, resulting in an immutable audit trail that guarantees transparency and accountability.

This layer not only helps in enhancing the security of user identities but also enables regulatory compliance and user trust in the identity management system.[28,29]

a. IPFS Layer:
The IPFS (InterPlanetary File System) Layer is responsible for secure, decentralized storage of identity-related data,[30] including biometric feature vectors and sensitive documents. This mechanism assigns a unique cryptographic hash to each stored file, making it immutable and easily verifiable.[31] To maintain privacy and security, sensitive biometric data is encrypted before being stored in IPFS, making sure only authorized entities can access it. Additionally, only hashes (references) of stored files are recorded on the blockchain, preventing raw exposure of biometric data while preserving the auditability and integrity of records.

IPFS offers decentralized, content-addressable storage without long-term data availability guarantees. To solve for this, our system embraces a hybrid pinning approach. Biometric information is pinned using self-hosted IPFS nodes, providing high-fidelity control and free from third-party infrastructure dependency. Furthermore, certain records are redundantly pinned using commercial services like Pinata or Web3 storage for enhanced availability and geographic redundancy.[32]

This two-layer approach provides high availability while addressing IPFS's documented persistence shortcomings. A strict data retention policy is enforced: identity records are kept for at least five years or until a revocation request is logged. When revocation occurs, unpinning is initiated (subject to legal or regulatory considerations), and all pin/unpin actions are audit-logged.[33]

b. Neuro-Secure Authentication Mechanism
The neuro-secure authentication mechanism or *N-SAM* is a hybrid biometric identity verification framework[34] that integrates biometric authentication, deep learning based neural networks, smart contracts and encryption systems to seamlessly authenticate users while ensuring a tamper resistant, privacy preserving platform, enhancing both security and trust.

a. Biometric data preprocessing & feature extraction: At the heart of N-SAM is its biometric processing system that draws out distinctive biometric features of users, mainly facial recognition for verification. When a user tries to sign-in, the face image is taken and preprocessed for enhanced recognition accuracy.

The system extracts facial embeddings using pretrained models accessed via the DeepFace library,[35] which provides a unified interface to several state-of-the art face recognition models. Specifically, we used three pretrained models: FaceNet, FaceNet512, and ArcFace.

Both FaceNet variants are based on the InceptionResNetV1 architecture and trained using triplet loss, which optimizes the embedding space to bring same-identity pairs closer while pushing apart different-identity pairs, FaceNet512 differs in embedding size, offering higher-dimensional representations for potentially improved separability.[36]

ArcFace,[37] on the other hand, is built on a ResNet100 backbone and uses Additive Angular Margin Loss which enforces angular margins between classes in the embedding space. This results in high inter-class separability and intra-class compactness—making ArcFace particularly effective for face verification tasks.

Tables 1 and 2 depicts the resultant analysis of these models, while Figure 2 displays the Receiver Operating Characteristic (ROC) curves across all folds.

To evaluate model performance in a standardized setting, we benchmarked all three models on the Labeled Faces in the Wild (LFW)[38] dataset using the standard evaluation protocol. We utilized the official LFW "10_folds" test set obtained via scikit-learn's fetch_lfw_pairs function,[39] which provides 6,000 pre-defined pairs (3,000 genuine and 3,000 impostor pairs) derived from the dataset's 13,233 images of 5,749 individuals. This standardized test set ensures reproducibility and enables direct comparison with published results. Following the standard LFW protocol, we

DOI: https://doi.org/10.70389/PJS.100142 | Premier Journal of Science 2025;15:100142

Table 1 | LFW evaluation analysis

Model	Best Threshold	Accuracy (Mean ± SD)	FAR (Mean ± SD)	FRR (Mean ± SD)	AUC (Mean ± SD)	EER (Mean ± SD)
FaceNet	0.6063	0.9682 ± 0.0054	0.0178 ± 0.0039	0.0180 ± 0.0038	0.9927 ± 0.0031	0.0179 ± 0.0038
FaceNet512	0.5788	0.9765 ± 0.0043	0.0128 ± 0.0029	0.0130 ± 0.0032	0.9964 ± 0.0016	0.0129 ± 0.0031
ArcFace	0.7137	0.9697 ± 0.0051	0.0182 ± 0.0029	0.0180 ± 0.0029	0.9935 ± 0.0025	0.0181 ± 0.0029

Table 2 | BUPT evaluation analysis

Model	Best Threshold	Accuracy (Mean ± SD)	FAR (Mean ± SD)	FRR (Mean ± SD)	AUC (Mean ± SD)	EER (Mean ± SD)
FaceNet	0.6823	0.9415 ± 0.0083	0.0315 ± 0.0049	0.0325 ± 0.0049	0.9802 ± 0.0051	0.0320 ± 0.0048
FaceNet512	0.6646	0.9542 ± 0.0099	0.0252 ± 0.0057	0.0253 ± 0.0058	0.9883 ± 0.0039	0.0253 ± 0.0057
ArcFace	0.7907	0.9342 ± 0.0116	0.0358 ± 0.0047	0.0358 ± 0.0049	0.9771 ± 0.0068	0.0358 ± 0.0048

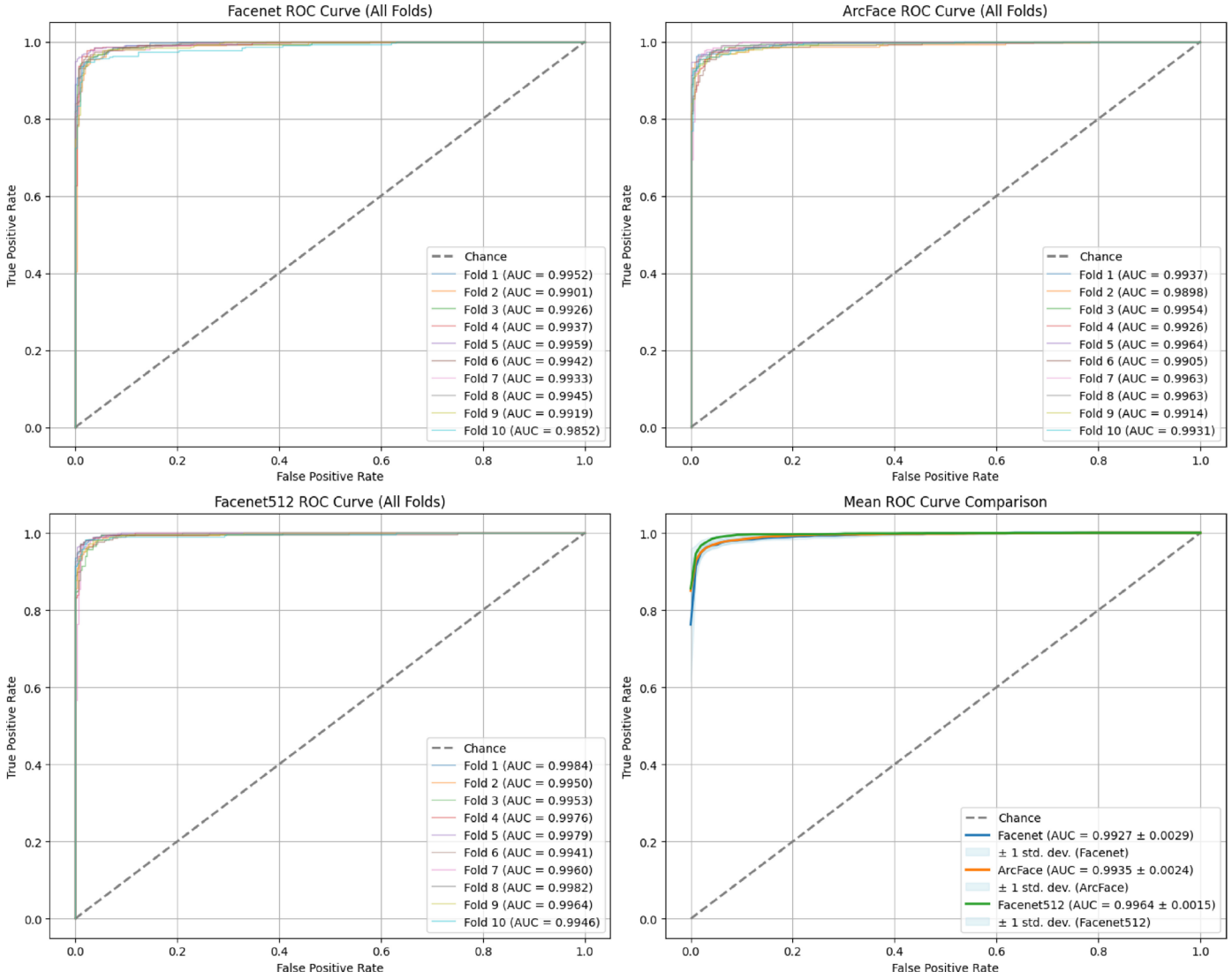

Fig 2 | ROC Curves for FaceNet, ArcFace, FaceNet512 and the mean comparison of the three

employed 10-fold cross-validation with the official fold splits, where each fold contains 600 pairs (300 genuine, 300 impostor). Subjects may appear in multiple pairs across folds, as per the standard LFW evaluation design, genuine pairs are drawn from the subset of 1,680 individuals with multiple images, while impostor pairs utilize the full set of 5,749 individuals. For each fold, cosine similarity between the face embeddings was computed for every pair.

To find the optimal operational point, we performed a threshold sweeping analysis. This involved iterating through 1000 thresholds, ranging from the minimum to the maximum computed distance. At each threshold, we classified pairs as a match or non-match and calculated the accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR). The optimal threshold was selected as the one that achieved the highest accuracy. This rigorous method ensures that the reported metrics are based on the most effective performance of each model.

To complement the LFW evaluation and assess model robustness on more challenging data, we additionally evaluated all three models on the BUPT-CBFace dataset, which contains 41,667 identities with 12 images per identity, representing a significantly larger and more diverse set than LFW's 5,749 identities. Due to the dataset's size, we sampled 6,000 pairs (3,000 genuine and 3,000 impostor) following the same distribution as our LFW evaluation. Genuine pairs were created by randomly selecting different images from the same identity, while impostor pairs were formed from images of different identities. The sampled subset maintains the dataset's inherent diversity in pose, expression, and imaging conditions, providing a more challenging evaluation scenario.

We applied the identical evaluation protocol used for LFW: 10-fold cross-validation with 600 pairs per fold, cosine similarity computation, and the same threshold sweeping analysis across 1,000 thresholds to determine optimal operational points. This consistent methodology enables direct comparison between the two datasets and demonstrates model generalization beyond the relatively constrained LFW benchmark. As expected, all models showed reduced performance on BUPT-CBFace (Table 2), confirming its increased difficulty while demonstrating that our approach maintains robust performance across diverse conditions.

Tables 1 and 2 show the analysis results for LFW and BUPT-CBFace respectively, while Figure 2 compares the Receiver Operating Characteristic (ROC) curves. To illustrate threshold effects, we plot True Positive Rate (TPR) versus False Positive Rate (FPR) across thresholds for each model. The top two and bottom-left subplots show ROC curves for the 5 cross-validation folds of FaceNet, ArcFace, and FaceNet512, with AUC reported per fold. The bottom-right subplot compares the mean ROC curves of all models, with shaded areas indicating standard deviations and AUC reflecting overall performance.

Based on Table 1, FaceNet512 offers the best overall performance with the highest accuracy (97.65% ± 0.43%), making it the most reliable among the three at its optimal threshold of 0.5788.

b. Decentralized identity verification:
To ensure decentralization and privacy, the Content Identifier (CID) of the biometric data stored in the IPFS layer is encrypted and stored on-chain. The CID is linked with the User's Decentralized Identifier (DID), enabling secure and efficient mapping between users and their biometric data.

During a sign-in procedure, the following steps occur:

- The user's DID (which, in general blockchain systems, would be a wallet address) is captured along with the newly acquired biometric facial data.
- The biometric data undergoes the same preprocessing and feature extraction steps described earlier to generate feature vectors.
- The CID is used to retrieve the original biometric features from the IPFS, which are decrypted after user confirmation.
- A cosine similarity is performed between the stored feature vectors and the newly extracted feature vectors.
- If the similarity score exceeds a predefined authentication threshold, the user is successfully authenticated.

c. Blockchain Implementation:
Using a distributed ledger technology, blockchain in this case, allows us to decentralize all identity information and makes access transparent.

Smart Contracts are defined to maintain access control, permission requests and overall user control on their data. A smart contract is a piece of code that is executed in a secure environment enabling the user to control digital assets.[9] It can include various methods to automatically execute the terms of the agreement between participants of the chain thus removing the need for an unnecessary intermediary or delays. In this particular project, the smart contract provides functions for users to register their decentralized identifier on the blockchain, user authentication off-chain, access control and a logging/audit trail. The smart contract functions, parameters and estimated gas costs involved are provided in the supplementary material as Table S1.

User registration will generate a unique identity token after storing the hashed biometric data securely off-chain. Access control is maintained through grantAccess, revokeAccess and checkAccess methods as shown in Table S1. These methods are able to control whether a third entity can access a certain user's data for some time frame. This access can also be revoked or checked at any time so that the user always maintains full transparent control over their personal information.

All accesses will also be logged with the logAccess method and its corresponding emitted event. This maintains a public record of which entity accessed what data, further encouraging blockchain principles of transparency.

Every function within the smart contract operates at O(1) complexity, meaning gas costs remain constant

DOI: https://doi.org/10.70389/PJS.100142 | Premier Journal of Science 2025;15:100142

regardless of user base growth. Thus, transaction fees remain predictable with great scalability potential.[40] However, it's important to note that while the contract logic scales efficiently, overall system throughput still faces limitations based on the network capacity and deployment architecture.

The consensus mechanism used in this project is Proof of Authority (PoA) due to the vulnerability of digital identity and its implications if scaled. Nodes on the blockchain are only validated by trusted organizations, likely government agencies or large reputed groups. Validators are always a fixed set of authorized nodes and are called sealers.

The PoA consensus mechanism was selected for this system due to its optimal balance of security, efficiency, and trust requirements. Unlike Proof of Stake (PoS) which requires significant cryptocurrency holdings or Delegated Proof of Stake (DPoS) which introduces democratic but potentially vulnerable election processes, PoA leverages the reputation of validators whose identities are known and vetted.[27,41] This approach is particularly suitable for digital identity management where trust and accountability are paramount. Additionally, PoA provides enhanced security against 51% attacks since compromising the network would require controlling the majority of trusted validator nodes rather than simply accumulating computational power or stake.[27]

As a result, the validators are chosen to be large, trusted organizations or government agencies whose identities are extremely difficult to reproduce. This category of validators inherently mitigates the danger of validator collusion or a Sybil attack, further enhanced by promoting diversity in chosen nodes. A system implementation on a national scale would accommodate this validator criteria. Selection can be done through invites based on established credibility and technical capabilities. Besides that, the organization must possess significant resources to contribute to the network and also technical capabilities considering the workings of a blockchain system.

d. Security Mechanism

As biometric information is stored off-chain, all identifiers linking to it must be securely encrypted using symmetric encryption. This includes biometric or identity-related documents where Advanced Encryption Standard (AES) can be implemented for efficiency before being stored on the IPFS. This prevents malicious actors from accessing the information even if the IPFS link is exposed.[42] The encryption key is further secured through Elliptic Curve Cryptography (ECC), a method of asymmetric encryption.[43] This ensures only the intended user can decrypt the data, essentially, the original owner.

Third party access is made possible through re-encrypting the key using the third party's public key and correspondingly updating the smart contract. Thus the intended entity and only them can retrieve the original document. To enforce data control for the user, access revocation is also enabled on chain through the Smart Contract. This is implemented by removing or updating encrypted keys which ensure that previously granted access becomes nullified and prevents unauthorized access beyond that point.[43]

Deep learning techniques have also been researched to assist in identifying forgery, malicious tampering and other modifications which could potentially be incorporated in the future.[44]

e. Recovery Mechanisms

The potential loss of biometric keys must be addressed for long term viability of the system and overall user friendliness. This challenge is tackled through a guardian assisted recovery mechanism, which allows users to designate trusted individuals or entities as guardians for their digital identity. The addGuardian function in the smart contract shown in Table S1 are relevant here. Users can assign guardians through the addGuardian function enables a guardian to reset a user's identity as a secure fallback option.

f. GDPR and Ethics

The General Data Protection Regulation (GDPR) presents a significant challenge for blockchain-based identity systems, particularly concerning the right to erasure (Article 17). This right allows individuals to request the deletion of their personal data, which conflicts with blockchain's fundamental principle of immutability.[45] Our architecture attempts to address this challenge through the following measures through off-chain IPFS storage of biometric data and one-way hashing.

As mandated by GDPR, a Data Protection Impact Assessment (DPIA)[46] would be essential prior to any production deployment of this system. The DPIA process enables systematic identification and mitigation of risks to data subjects, especially regarding storage, processing, and potential misuse of biometric data. For architectures of this kind, DPIA documentation should include privacy risk assessments, technical and organizational controls, and records of residual risk, prepared before onboarding users and updated during substantial system changes. Referencing DPIA requirements here ensures regulatory accountability and supports legal defensibility for biometric-storage and credential-management activities, although a formal DPIA is not prepared or submitted as part of this work.

One of the concrete technical methods to mitigate this issue is through encrypted revocation registries. This is implemented with an off-chain encrypted registry maintaining erasure requests and corresponding cryptographic proof. On invoking their right to erasure, the system generates a revocation certificate that must be validated by PoA validators and is stored in the registry.

Additionally, chameleon hashes[47] can be proposed for on-chain identity records instead of

standard cryptographic hashes. These trapdoor hash functions allow authorized validators to selectively update hash values referencing biometric records, for example by substituting pointers to deleted data with standardized "erased" markers in compliance with GDPR erasure requests. Importantly, chameleon hashing achieves a controlled and auditable form of mutability: only those parties possessing the trapdoor key (typically trusted validators) can perform rewrites, and all such modifications are recorded in on-chain logs. This approach does not compromise the overall immutability and integrity of the blockchain ledger; the underlying chain remains append-only, and all changes are traceable and non-repudiable. By enabling legally mandated data modifications without undermining the core principles of distributed consensus and auditability, chameleon hashes reconcile the tension between regulatory compliance (e.g., GDPR Article 17) and the immutability required by permissioned blockchains.

However, it's important to acknowledge the limitations of this approach. While the actual data can be deleted from IPFS, the hashes (CIDs) stored on the blockchain remain immutable. This creates a persistent link, albeit encrypted, to the original data location. Achieving complete erasure in a decentralized system remains challenging, as data may be replicated across multiple nodes.

Biometric data misuse is a significant ethical concern. This is mitigated by strict validator criteria based on reputation, credibility and dependency on public opinion. These nodes are generally government agencies or large trusted organizations, so the danger of data misuse is limited.[48]

g. Demographic Bias in Face Recognition:
Face recognition models, including FaceNet512, can exhibit demographic differentials, leading to uneven performance across age, gender, and ethnic groups. While our current system uses the LFW dataset for benchmarking, we acknowledge this limitation for real-world deployment. Future mitigation strategies include:

- *Diverse and Balanced Datasets:* Train models on more demographically representative datasets to ensure equitable performance.
- *Multimodal Biometrics:* Integrate alternative authentication methods (e.g., fingerprint, iris, voice) to provide fallback options for users disproportionately affected by facial recognition bias.
- *Fairness-Aware Thresholding:* Implement adaptive thresholds to minimize unequal false acceptance/rejection rates across demographic groups.
- *Fairness Audits and Metrics:* Conduct independent audits using fairness metrics to monitor and correct demographic disparities.

These measures collectively ensure that the system remains ethical, inclusive, and responsible, addressing both privacy and fairness challenges especially in the case of demographic bias.

h. Formal Security Analysis using STRIDE Framework
Using the STRIDE framework, we can analyze the system's security against various threats.

- *Spoofing:* Template inversion attacks can be mitigated through one-way feature extraction with the neural networks. The FaceNet512 model embeddings cannot be reverse-engineered to reconstruct the original data.[36] The high accuracy with low FAR results show resistance to spoofing attempts.
- *Tampering:* Blockchain immutability prevents modifying identity records and the IPFS implementation ensures data integrity through cryptographic hashes.
- *Repudiation:* The logAccess function ensures that all authentication attempts are logged on-chain, creating an immutable audit trail. These events provide evidence of access requests and grants.
- *Information Disclosure:* Biometric templates are encrypted using AES before IPFS storage, with keys further encrypted with ECC. Only hashed CIDs are stored on-chain, not raw biometric data.
- *Denial of Service:* The PoA consensus limits validator nodes to only reputable and trusted entities, reducing DoS attack vectors. Moreover, IPFS is a distributed storage which inherently prevents single points of failure and the smart contract is optimized to O(1) complexity, maintaining consistent performance under load.
- *Elevation of Privilege:* The guardian recovery system includes multi-signature requirements preventing unauthorized escalation. PoA validators are public, trusted and reputable organizations, mitigating Sybil attacks and validator collusion through reputation based selection.

Results and Discussion

The proposed Neuro-Secure Blockchain identity management system brings together decentralization of digital identity alongside biometric authentication to address limitations of traditional systems. Compared to centralized architectures which are vulnerable to data breaches and identity theft,[2] this model ensures identity records are distributed across a blockchain network and biometric data is stored in encrypted and hashed form.

The reliance on third-party providers is removed and transfers complete control over identity verification and access permission to the data owner. Blockchain introduces computational overhead but this approach minimizes on-chain storage using IPFS for document and biometric data storage. Thus, a hybrid model for storage optimizes operational and computational costs.[43]

Security analysis of the smart contract was done using Mythril, a smart contract verification tool that uses Bytecode analysis to detect vulnerabilities and assigns severity levels to each.[49] This analysis

DOI: https://doi.org/10.70389/PJS.100142 | Premier Journal of Science 2025;15:100142

returned no vulnerabilities as further explained within Appendix A of the supplementary material.

Quantitative Evaluation and Comparative Analysis

This section presents a comparative evaluation between the proposed decentralized biometric authentication system and traditional centralized approaches. Key metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), end-to-end authentication latency, and storage overhead are examined. Centralized system benchmarks are drawn from reported values in existing literature, while the decentralized system's values are based on tests conducted on a standard consumer-grade machine.

Comparison with Centralized Biometric Systems

Table 3 depicts the differences between FaceNet512 and other biometric systems based on FAR, FRR and the dataset used. The results in Table 3 indicate that the proposed decentralized system using FaceNet512 delivers competitive performance when compared to centralized biometric systems. With a FAR of 1.5%, it demonstrates reliable accuracy and aligns well with, the benchmarks set by traditional approaches.

Table 3 | Quantitative comparisons with centralized systems

Research Paper	System/ Technique	Dataset Used	FAR (%)	FRR (%)
[54]	Gabor-LBP	Newly collected (indoor office)	0.28	8.5
[54]	Modified Gabor-LBP	Newly collected (indoor office)	0.0	5.0
[55]	CNN-based room security system	Facial dataset (CNN model)	26.67	9.33
[56]	Various algorithms (IJB-A benchmark)	IARPA Janus Benchmark–A (IJB-A)	1.0	3.9
This Paper	FaceNet512	LFW	1.5	1.5

Storage Cost Comparison with PKIs

Table 4 shows the comparison between centralized PKI and the decentralized model which highlights the cost-efficiency and scalability advantages of the decentralized biometric system.

With significantly lower storage costs, no compliance audit overhead, and native support for geographic redundancy via IPFS, the decentralized model demonstrates strong potential as a lightweight and scalable alternative to traditional PKI-based solutions.[50–53]

Table 5 provides a high-level architectural comparison of our proposed system with existing state-of-the-art SSI frameworks, highlighting differences in DID/VC standards, privacy, biometric support, scalability, storage, governance, and interoperability.[5,7,14]

Table 4 | Cost comparison table

Metric	Centralized PKI	Decentralized Model
Storage Cost/ User/Month	$4.20-$8.50	$0.008-$0.02
Compliance Audits	$10k+/year	Audit-free architecture
Geographic Redundancy	30% cost premium	Built-in via IPFS
Scalability Threshold	50k users @ $182k/yr	1M users @ $80/month

Scalability Evaluation

End-to-end authentication latency was measured on consumer hardware (8GB RAM, Intel i5 Processor) and averaged 4.028s for registration and 1.069s for verification, including biometric processing and IPFS operations. These registration processes involved face capture, embedding generation, encryption and IPFS upload. The verification process involved face capture, embedding generation, IPFS fetch, decryption and comparison.

A scalability evaluation was conducted on a 7-validator PoA testnet deployed across separate instances on a local network. The experiment processed 22,677 identity transactions and achieved 31.5 TPS (Transactions per Second) average throughput with 44.79 TPS peak performance and 99.61% success rate at 5-second block intervals.

Table 5 | Architectural comparison with other frameworks

Feature	Hyperledger Indy/Sovrin	Microsoft ION	BIO-SSI	Our System
DID/VC	Partial (AnonCreds, ZKPs)	Full (W3C VC, DID)	Partial to full support with biometric extensions	Full (W3C VC, DID, IPFS)
Privacy	High (Pairwise DIDs, ZKPs)	High (Selective Disclosure)	High (with encryption, privacy-preserving matching)	High (biometrics + AES, ECC)
Biometric Support	Low	Medium (ZKP-based, no on-device)	High (NN-based verification)	High (NN templates, privacy-preserving)
Scalability	Medium (permissioned)	High (public, permissionless)	High (public, permissionless)	High (hybrid IPFS/PoA)
Storage	On-chain credential refs, some off-chain	Off-chain encrypted anchors	Hybrid: biometric data encrypted and stored off-chain, blockchain anchor	Hybrid: IPFS (biometrics), blockchain hashes
Governance	Consortium-based (Linux Foundation)	Public open network	Consortium/permissioned	PoA with trusted validators
Interoperability	Medium	High (W3C compliant)	Medium	High (W3C compliant)

Block propagation analysis across validators showed average latency of 103 ms with 95th percentile at 119 ms. Five failure scenarios tested network resilience; single validator failures caused minimal impact (8% performance reduction, 12s recovery), minority failures (3/7 validators) reduced throughput by 28% with 35s recovery. Network partitions and cascading failures severely impacted performance (65–85% reduction, up to 145s recovery), while Byzantine faults showed 28% performance impact with maintained consensus.

Storage growth on-chain is 0.58 MB per 1,000 transactions, and the storage growth off-chain (IPFS) is approximately 2170 bytes/user considering FaceNet512 embedding sizes and additional encryption metadata.[36]

Strategic Implementation Framework and Protocol Integration Plan

A hybrid implementation strategy allows concurrent operation of traditional identity systems and decentralized mechanisms during the transition period.[3] Based on the blockchain implementation principles described in our research, the recommended implementation timeline encompasses these phases:

1. Initial validation period (0–6 months): Controlled deployment within a limited user cohort (e.g., internal development teams) enables testing of biometric credential issuance, selective disclosure protocols, and middleware integration with existing authentication frameworks.[57] Findings from this phase inform protocol refinements before broader implementation.
2. Transitional implementation (6–18 months): Expanded deployment across diverse user segments while maintaining conventional authentication alternatives. Integration middleware facilitates standardized workflows (e.g., OpenID Connect (OIDC) token generation via blockchain verification).[22] This phase emphasizes usability assessment and gradual introduction of Verifiable Credentials for specific processes.
3. Expanded deployment (18–36 months): Integration with external partner systems and third-party applications. Authentication policies may designate DID-based mechanisms as primary verification protocols. Systems begin implementing decentralized trust frameworks and Proof of Authority (PoA) validator nodes as fundamental identity components.[21]
4. Comprehensive integration (36+ months): Decentralized authentication becomes the predominant verification methodology. Legacy systems remain accessible through protocol conversion interfaces for backward compatibility but undergo systematic deprecation.[4] This phased implementation strategy minimizes operational disruption while enabling iterative enhancements.

Conclusion

The Neuro-Secure blockchain-based identity management system could represent a significant advancement in digital identity verification, addressing critical vulnerabilities in centralized identity systems. By integrating blockchain technology with neural network biometric authentication, the research provides a secure, privacy-preserving alternative that shifts control of digital identities from centralized authorities to individual users.

The Neuro-Secure Digital Identity Management system aligns with emerging trends in Self-Sovereign Identity (SSI), Web3 decentralization principles, and zero-trust security models,[24] offering a comprehensive solution to critical challenges in digital identity verification. The system demonstrates how blockchain and advanced AI can effectively secure personal identity data, offering enhanced privacy and user control through decentralized verification mechanisms. Key contributions include a novel approach to biometric authentication that preserves individual sovereignty while providing security against identity theft and unauthorized data access.

Practical implications span multiple sectors, including financial services, healthcare, government, and education, showcasing the potential for widespread adoption of decentralized identity management.[58]

Future research directions include focusing on advancing machine learning models for biometric authentication, exploring enhanced zero-knowledge proof implementations, developing multimodal biometric authentication techniques, and developing cross-blockchain interoperability. Ultimately, the Neuro-Secure system represents a pivotal step towards a digital ecosystem where individuals have genuine control over their personal data, combining technological innovation with a fundamental respect for personal privacy.

References

1 J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," Business & Information Systems Engineering, 2021;63(5): 603–613. https://doi.org/10.1007/s12599-021-00722-y

2 H. Li, Y. Jing, and Z. Guan, "The Review and Comparison between Centralized and Decentralized Digital Identity Systems," Mobile Information Systems, 2024:1–10. https://doi.org/10.1155/2024/6651273

3 A. M. Buttar, M. A. Shahid, M. N. Arshad, and M. A. Akbar, "Decentralized Identity Management using Blockchain Technology: Challenges and solutions," in Signals and communication technology, 2024:131–166. https://doi.org/10.1007/978-3-031-49593-9_8

4 P. Herbke, T. Cory, and M. Migliardi, "Decentralized Credential Status Management: A paradigm shift in digital trust," arXiv (Cornell University), Jun. 2024, 1. https://doi.org/10.1109/BRAINS63024.2024.10732832

5 R. A. Pava, J. M. Such, and V. M. Álvarez, "Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation," Frontiers in Blockchain, 2024;7. https://doi.org/10.3389/fbloc.2024.1443362

6 E. Krul, H.-Y. Paik, S. Ruj, and S. S. Kanhere, "SoK: Trusting Self-Sovereign Identity," arXiv preprint, Apr. 2024,.https://doi.org/10.56553/popets-2024-0079

7 Y. Yasumura, M. Fujio, W. Nakamura, and K. Takahashi, "Bio-SSI: Self-Sovereign Identity Bound to Biometrics," in Proceedings of the IEEE Cyber Science and Technology Congress (CyberSciTech), 2024:369–377. https://doi.org/10.1109/CyberSciTech64112.2024.00064

8 A. Panch and M. Agarwal, "Deep Feed-Forward Neural Network-Based Biometric Authentication System with Biometric Identity

and Reputation Score in Blockchain," Journal of Biometric Security, 2024;9(3):55–71, https://doi.org/10.1142/S1469026824500196
9 A. Kumar, A. Paliwal, B. Tanwar, G. Maheshwari, and S. Maheshwari, "Harnessing Blockchain and Smart Contracts for Next-Generation Digital Identity: Enhancing Security and Privacy," International Journal for Research in Applied Science and Engineering Technology (IJRASET), 2025;67(4):1234–1245. https://doi.org/10.22214/ijraset.2025.67058
10 S. Islam and K. U. Apu, "Decentralized vs. Centralized Database Solutions In Blockchain: Advantages, Challenges, and Use Cases," Global Mainstream Journal of Innovation, Engineering & Emerging Technology., 2024;3(4):58–68. https://doi.org/10.62304/jieet.v3i04.195
11 C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," IEEE Communications Surveys & Tutorials, 2025:1, https://doi.org/10.1109/COMST.2025.3543197
12 "Home - EBSI -," Aug. 25, 2001. https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/447687044/Home
13 European EPC Competence Center GmbH (EECC) et al., Empowering Sustainable Products and Consumer Confidence through Verifiable Credentials. 2023. [Online]. Available: https://www.gs1-germany.de/fileadmin/gs1/fachpublikationen/whitepaper-idunion-case-study-gs1-germany.pdf
14 S. Aggarwal and N. Kumar, "Hyperledger," in Advances in computers, 2020, pp. 323-343. https://doi.org/10.1016/bs.adcom.2020.08.016
15 Y. Liu, J. She, J. Zhao, F. Wang, and S. Kawata, "An Improved-PoA Consensus Algorithm for Blockchain-empowered Data Sharing System," in Proceedings of the Conference on Trust, Privacy and Security in Digital Business, Sep. 2022, pp. 45–59, https://doi.org/10.1145/3559795.3559813
16 H. Moniz, "The Istanbul BFT Consensus Algorithm," arXiv (Cornell University), Jan. 2020,
17 J. Kwon, Tendermint : Consensus without mining. Semantic Scholar, 2014. [Online]. Available: https://www.semanticscholar.org/paper/Tendermint-:-Consensus-without-Mining-Kwon/df62a45f50aac8890453b6991ea115e996c1646e
18 H. Otroshi Shahreza 1 et al., "Hybrid protection of biometric templates by combining homomorphic encryption and cancelable biometrics," journal-article, 2021. [Online]. Available: https://publications.idiap.ch/downloads/papers/2022/OtroshiShahreza_IJCB_2022.pdf. https://doi.org/10.1109/IJCB54206.2022.10007960
19 S. M. Abdullahi, S. Sun, B. Wang, N. Wei, and H. Wang, "Biometric template attacks and recent protection mechanisms: A survey," Information Fusion, vol. 103, p. 102144, Nov. 2023, https://doi.org/10.1016/j.inffus.2023.102144
20 N. Yuvaraj, T. Preethi, A. C. Sumathi, and K. R. S. Preethaa, "Alzheimer disease classification based on multimodel deep convolutional neural network using MRI images," AIP Conference Proceedings, vol. 2899, p. 060008, Jan. 2023, https://doi.org/10.1063/5.0144082
21 D. Mohanapriya, P. Mathivanan, M. Chairman, N. S. Sakthi, S. Sathish, and R. Dhilip, "Federated Learning and Biometric Identification for Continuous User Authentication Using Hybrid Neural Models," Journal of Information Systems Engineering and Management, 2025;10(26):1–8 https://doi.org/10.52783/jisem.v10i26s.4275
22 F. Liu, Z. Zheng, Y. Shi, Y. Tong, and Y. Zhang, "A survey on federated learning: a perspective from multi-party computation," Frontiers of Computer Science, vol. 18, no. 1, Dec. 2023, https://doi.org/10.1007/s11704-023-3282-7
23 G. Pradel and C. J. Mitchell, "Privacy-preserving biometric matching using homomorphic encryption," in Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, Oct. 2021, pp. 494–505. https://doi.org/10.1109/TrustCom53373.2021.00079
24 S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," Aug. 2020. https://doi.org/10.6028/NIST.SP.800-207
25 N. Daswani and M. Elbayadi, "The Equifax breach," in Apress eBooks, 2021, pp. 75–95. https://doi.org/10.1007/978-1-4842-6655-7_4
26 N. Mansoor, K. F. Antora, P. Deb, T. A. Arman, A. A. Manaf, and M. Zareei, "A review of Blockchain Approaches for KYC," IEEE Access, vol. 11, pp. 121013–121042, Jan. 2023, https://doi.org/10.1109/ACCESS.2023.3328536
27 S. Joshi, "Feasibility of proof of authority as a consensus protocol model," arXiv (Cornell University), Jan. 2021,
28 A.-E. Panait, R. F. Olimid, and A. Stefanescu, "Identity Management on Blockchain – privacy and security aspects," arXiv (Cornell University), Jan. 2020,
29 B. Faber, G. C. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS:A blockchain-based personal data and Identity management system," Proceedings of the ... Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii International Conference on System Sciences, Jan. 2019, https://doi.org/10.24251/HICSS.2019.821
30 J. Benet, "IPFS – Content Addressed, Versioned, P2P File system," arXiv (Cornell University), Jan. 2014,.
31 S. C, V. R. Falmari, and B. M, "Secure IoT-enabled sharing of digital medical records: An integrated approach with reversible data hiding, symmetric cryptosystem, and IPFS," Internet of Things, vol. 24, p. 100958, Oct. 2023, https://doi.org/10.1016/j.iot.2023.100958
32 J. Swati and P. Nitin, "Securing decentralized storage in Blockchain: a hybrid cryptographic framework," Cybernetics and Information Technologies, vol. 24, no. 2, pp. 16–31, Jun. 2024, https://doi.org/10.2478/cait-2024-0013
33 Y. Du, H. Duan, A. Zhou, C. Wang, M. H. Au, and Q. Wang, "Enabling secure and efficient decentralized storage auditing with blockchain," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3038–3054, May 2021,.https://doi.org/10.1109/TDSC.2021.3081826
34 N. D. Sarier, "Efficient biometric-based identity management on the Blockchain for smart industrial applications," Pervasive and Mobile Computing, vol. 71, p. 101322, Dec. 2020, https://doi.org/10.1016/j.pmcj.2020.101322
35 Serengil, "GitHub - serengil/deepface: A Lightweight Face Recognition and Facial Attribute Analysis (Age, Gender, Emotion and Race) Library for Python," GitHub. https://github.com/serengil/deepface
36 F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2015, pp. 815–823, Jun. 2015, https://doi.org/10.1109/CVPR.2015.7298682
37 J. Deng, J. Guo, J. Yang, N. Xue, I. Kotsia, and S. Zafeiriou, "ARCFaCE: Additive angular margin loss for deep face recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 10, pp. 5962–5979, Jun. 2021, https://doi.org/10.1109/TPAMI.2021.3087709
38 G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A database for studying face recognition in unconstrained environments." [Online]. Available: http://tamaraberg.com/papers/lfw.pdf
39 "fetch_lfw_pairs," Scikit-learn. https://scikit-learn.org/stable/modules/generated/sklearn.datasets.fetch_lfw_pairs.html
40 A. A. Zarir, G. A. Oliva, Z. M. Jiang, and A. E. Hassan, "Developing Cost-Effective Blockchain-Powered Applications," ACM Transactions on Software Engineering and Methodology, vol. 30, no. 3, pp. 1–38, Mar. 2021,.https://doi.org/10.1145/3431726
41 Shifferaw, Y., & Lemma, S. (2021). Limitations of proof of stake algorithm in blockchain: A review. Zede Journal, 39(1), 81–95
42 M. Ali, I. a. A. El-Moghith, M. N. El-Derini, and S. M. Darwish, "Wireless Sensor Networks Routing Attacks Prevention with Blockchain and Deep Neural Network," Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 70, no. 3, pp. 6127–6140, Oct. 2021, https://doi.org/10.32604/cmc.2022.021305
43 S. Jadhav, G. Choudhari, M. Bhavik, R. Bura, and V. Bhosale, "A Decentralized Document Storage Platform using IPFS with Enhanced Security," 2022 6th International Conference on Computing, Communication, Control and Automation (ICCUBEA, pp. 1–11, Aug. 2024, https://doi.org/10.1109/ICCUBEA61740.2024.10774730
44 P. Blessy, K. Kathiresan, and N. Yuvaraj, "Deep Learning approach to offline signature Forgery Prevention," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1570–1575, Mar. 2023,.https://doi.org/10.1109/ICACCS57279.2023.10112906
45 "Art. 17 GDPR - Right to erasure ('right to be forgotten') - General Data Protection Regulation (GDPR)," General Data Protection

Regulation (GDPR), Jun. 12, 2017. https://gdpr-info.eu/art-17-gdpr/
46 B. Wolford, "Data Protection Impact Assessment (DPIA)," GDPR.eu, Mar. 08, 2019. https://gdpr.eu/data-protection-impact-assessment-template/
47 A. Zafar, "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways," Journal of Cybersecurity, vol. 11, no. 1, Jan. 2025, https://doi.org/10.1093/cybsec/tyaf002
48 M. Ghafourian et al., "Combining Blockchain and Biometrics: A survey on technical aspects and a first legal analysis," arXiv (Cornell University), Jan. 2023, https://doi.org/10.48550/arxiv.2302.10883
49 M. A. Lateef and A. Kavitha, "Blockchain Smart Contract Fortification using Bytecode Analysis to Address Vulnerabilities," in CRC Press eBooks, 2024, pp. 87–90. https://doi.org/10.1201/9781003581215-18
50 SEALWeb and SWIFT, "Understand the total cost of your PKI solution."
51 DIGICERT, "Comparing cost of ownership: Trust Lifecycle Manager vs. on-premise software." [Online]. Available: https://www.digicert.com/content/dam/digicert/pdfs/whitepaper/comparing-cost-ownership-whitepaper-en.pdf
52 "Pinata | Pricing." https://pinata.cloud/pricing (accessed Apr. 08, 2025).
53 "Infuria | Pricing" https://www.infura.io/pricing (accessed Apr. 08, 2025)
54 H. Lee, S.-H. Park, J.-H. Yoo, S.-H. Jung, and J.-H. Huh, "Face recognition at a distance for a Stand-Alone access Control system," Sensors, vol. 20, no. 3, p. 785, Jan. 2020, https://doi.org/10.3390/s20030785
55 N. Sunardi, A. Fadlil, and D. Prayogi, "Room Security System Using Machine Learning with Face Recognition Verification," Revue D Intelligence Artificielle, vol. 37, no. 5, pp. 1187–1196, Oct. 2023, https://doi.org/10.18280/ria.370510
56 "IARPA Janus Benchmark – C: Face Dataset and Protocol," Noblis, [Online]. Available: https://noblis.org/wp-content/uploads/2018/03/icb2018.pdf
57 O. Delgado-Mohatar, J. Fierrez, R. Tolosana, and R. Vera-Rodriguez, "Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends," arXiv (Cornell University), Jan. 2020, doi: 10.48550/arxiv.2003.09262.
58 "Blockchain Technology Trends in Different Sectors: A review," Journal of Statistics Applications & Probability, vol. 13, no. 2, pp. 691–706, Nov. 2023, https://doi.org/10.18576/jsap/130209

Suplementary Material

Table S1 | Smart contract functions

Function name	Description	Parameters	Returns	Events Emitted	Estimated Gas	Cost (gwei)
Register Identity	Registers a user's decentralized identity by Storing a hashed biometric.	User (address), _biometric Hash (bytes32	None	None	~66668 gas	133.336
Update Identity	Updates the stored biometric hash for a user.	New Biometric Hash (bytes32)	None	Identity Updated (address_user)	~30617 gas	61.234
Verify Identity	Verifies if the given biometric hash matches the stored hash.	_user (address), _biometric Hash (bytes32)	Bool (true if access is valid)	Identity Verified (address_user, bool success)	~28868 gas	57.736
Grant Access	Grants temporary access to an entity for identity verification.	requester (address), _duration (uint256)	None	Access Granted (address_ user,address_requester, uint256 expirationTime)	~71393 gas	142.786
Revoke Access	Revokes access before expiration.	_requester (address)	None	Access Revoked (address_user, address_requester)	~29677 gas	59.354
Check Access	Checks if a requester has valid access.	_user (address), _requester (address)	bool (true if access is valid)	None	~38825 gas	77.765
Log Access	Logs authentication attempts on-chain.	_user (address), _requester (address), _timestamp (uint256), _success (bool)	None	Access Logged (address _user, address_requester, uint256_ timestamp, bool success)	~27758 gas	55.516
Add Guardian	Allows a user to assign a guardian for identity recovery.	_guardian (address)	None	Guardian Added (address_user, address_guardian)	~29364 gas	57.728
Remove Guardian	Removes a guardian assigned for recovery.	_guardian(address)	None	Guardian Removed (address_ user, address_guardian)	~29242 gas	58.484

[a]Gas estimates obtained using ethers.js with Ganache local block chain at 2 gwei gas price (April2025).
1 Gwei = 10−9 ETH; actual costs may vary based on network conditions.

Appendix A
Smart contract security verification outputs

A formal analysis was conducted on the proposed smart contract using Mythril v0.24.8 on the solidity version 0.8.29. The analysis was completed successfully and returned no security issues detected. Access control was verified and confirmed that only identity owners can modify their data, guardian functions are restricted to assigned guardians and time-bounded permissions are properly enforced.

Input validation was verified as all address parameters were checked for zero address, biometric hashes are non-Zero and access grant durations are with in acceptable limits. All state changes were verified to be atomic and consistent and properly logged via events without any unnecessary storage operations.

Moreover, the smart contract code is thoroughly documented using Solidity's Natural Language Specification Format (NatSpec) that includes descriptions of contract purpose, function behaviors, input parameters and expected return values. Additionally, Scribble assertions were incorporated to express key security properties and invariants within the contract thus enabling automated verification tools to check for correctness.

Listing A1 | Solidity codes Nippet with NatSpec and scribble assertions

```
/**
*@notice Registers a new decentralized identity using a biometric hash
*@dev Creates a new identity entry for the caller with the provided biometric hash
*@param_biometric Hash The cryptographic hash of the user's biometric data
*@custom: security The biometric hash should be generated using a secure hashing algorithm
*@custom: privacy The original biometric data should never be stored or transmitted
*
*Requirements:
*-Callermustnotalreadyhaveanidentityregistered
*-Biometrichashmustnotbezero
*
*Effects:
*-Creates new identity with exists=true and provided hash
*-No events emitted for privacy(registration is implicit)
*/
///#if_succeeds identities[msg.sender].exists==true
///#if_succeeds identities[msg.sender].biometric Hash==_biometric Hash {
///#if_succeeds identities[msg.sender].guardian==address(0) function register
Identity(bytes32 _biometric Hash) public {
///#require !identities[msg.sender].exists
///#require _biometric Hash!=bytes32(0)

require(!identities[msg.sender].exists, "Identity already registered"); require(_biometric
Hash != bytes32(0), "Invalid biometric hash");

User Identity storage new Identity=identities[msg.sender]; new Identity.biometric Hash =
_biometric Hash; new Identity.exists = true;
}
```


DOI: https://doi.org/10.70389/PJS.100142 | Premier Journal of Science 2025;15:100142