iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79483

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

DecentraID: A Blockchain-Based Self-Sovereign Identity System with Enhanced Privacy and Social Recovery

Anshita Rathore[1], Aayush Chouhan[2], Balraj Singh Randhawa[3], Mohd Affan Siddiqui[4], Dr. Abha Choubey[5]
[1, 2, 3, 4]*Student, Department of Computer Science and Engineering, Shri Shankaracharya Technical Campus, Bhilai*
[5]*Professor and HOD, Department of Computer Science and Engineering, Shri Shankaracharya Technical Campus, Bhilai*

Abstract: ***Digital identity systems continue to depend on centralized authorities that store, validate, and often monetize user data, creating persistent concerns related to privacy leakage, identity fraud, platform lock-in, and single points of failure. This paper presents DecentraID, a decentralized self-sovereign identity framework that combines Ethereum smart contracts, IPFS-based storage, client-side authenticated encryption, and W3C-aligned credential workflows to give users direct control over their digital identity records. In the proposed design, sensitive profile data and credential payloads are encrypted locally using AES-GCM before being uploaded to IPFS, while only content identifiers and verification metadata are anchored on-chain. The architecture also incorporates issuer-managed verifiable credentials and a guardian-based social recovery mechanism to reduce the risk of permanent identity loss caused by wallet or private-key compromise. Unlike conventional identity platforms that concentrate trust in a single provider, DecentraID distributes trust across cryptographic proofs, decentralized storage, and programmable smart contracts. Functional validation of the prototype on Ethereum Sepolia demonstrates secure profile registration, encrypted data retrieval, credential issuance and verification, revocation handling, and threshold-based recovery. The study shows that decentralized identity can be implemented in a way that is practical, privacy-aware, and extensible for academic, organizational, and e-governance use cases.***

Keywords: Self-Sovereign Identity, Blockchain, Ethereum, IPFS, Verifiable Credentials, AES-GCM, Social Recovery, Privacy.

I. INTRODUCTION

Digital identity has become a foundational requirement for participation in online systems, spanning education, finance, healthcare, public services, and social platforms. Yet the dominant identity model remains highly centralized. Users typically register on services that maintain full authority over identity records, authentication mechanisms, and access logs. This architecture simplifies administrative control, but it also produces a concentration of sensitive data that is attractive to attackers and difficult for users to audit or move across systems. Repeated incidents involving data leakage and identity misuse have exposed the structural weakness of this model rather than isolated implementation failures [1], [2].

Self-sovereign identity (SSI) has emerged as a response to these limitations. SSI shifts identity ownership toward the user by combining decentralized identifiers, portable credentials, and cryptographic verification. Instead of repeatedly surrendering personal data to centralized identity providers, users maintain a digital wallet or application that stores references to identity artifacts and presents verifiable claims only when needed [3], [4]. In this way, the holder gains stronger control over disclosure, provenance, and portability.

Blockchain technologies provide a natural trust anchor for SSI systems because they can store immutable records, policy rules, and revocation states without dependence on a single institution. However, a purely on-chain design is neither economical nor privacy preserving. Sensitive identity data should not be exposed on a public ledger, and storing large profile objects on-chain leads to substantial cost and scalability issues. As a result, modern decentralized identity architectures often combine blockchain for integrity and governance with off-chain storage for data persistence [5], [6].

DecentraID is developed within this design space. The system uses Ethereum smart contracts to register identity ownership, manage credential metadata, and execute recovery policies. IPFS is employed as the decentralized off-chain storage layer, while all sensitive data is encrypted on the client side before upload. The framework further supports W3C-style verifiable credentials and introduces guardian-based social recovery so that users are not permanently locked out if they lose access to their wallet [3], [7], [8].

The key contribution of this work is an integrated identity framework that emphasizes privacy by default, cryptographic verifiability, and practical recoverability. Instead of treating wallet loss as a terminal failure state, the proposed architecture embeds recovery logic as a first-class component. The result is a prototype that is not only technically decentralized but also more usable for real-world deployment in educational credentials, institutional verification, and secure onboarding scenarios.

II. LITERATURE REVIEW

Recent research on decentralized identity has focused on decentralized identifiers (DIDs), verifiable credentials (VCs), privacy-preserving disclosure models, and governance challenges. Mazzocca et al. provide a broad survey of DIDs and VCs, showing that standards-based identity systems are gaining traction across cloud, edge, IoT, and citizen-service settings, but they still face adoption challenges related to interoperability, wallet usability, and revocation management [4]. Pava-Diaz et al. compare prominent SSI frameworks and observe that many implementations only partially satisfy the broader principles of self-sovereignty, particularly with respect to recoverability, portability, and privacy control [9].

At the standards level, W3C DID Core formalizes a method-neutral model for decentralized identifiers, while the Verifiable Credentials Data Model defines portable, machine-verifiable attestations exchanged among issuer, holder, and verifier [3], [7]. These specifications are central to interoperable decentralized identity, but they do not prescribe a specific blockchain, storage, or wallet-recovery strategy. As a result, application-specific systems still need to solve problems related to key lifecycle management, encrypted data storage, and trust delegation. Blockchain-assisted SSI studies highlight the value of immutable attestations and tamper-resistant audit trails, especially in educational and institutional contexts. Chan reviews blockchain-assisted SSI in education and notes that user-centric records and portable attestations can reduce dependence on siloed academic databases while improving interoperability among institutions [10]. Hsieh et al. similarly demonstrate that SSI-based e-portfolio infrastructures can strengthen student data control and trust in digital achievement records [11].

Privacy remains a difficult concern because decentralized storage does not automatically imply confidentiality. Naicker et al. point out that many SSI deployments claim privacy benefits while still exposing metadata or lacking strong selective disclosure in practical workflows [12]. This motivates the use of client-side encryption, minimal on-chain exposure, and future support for zero-knowledge proofs. In the same direction, supervised and revocable privacy-preserving identity models have emphasized that attribute verification should reveal only what is needed rather than full credential contents [13].

Another persistent gap in decentralized systems is recovery. Standard wallet models make users solely responsible for their private keys, creating a major usability barrier. The ERC-7093 proposal addresses this by standardizing social recovery interfaces for smart contract accounts, allowing guardians and customizable recovery policies to participate in account restoration [8]. This idea directly informs the recovery component of DecentraID, which adapts guardian approval and delayed execution to identity ownership transfer. In summary, existing literature validates the promise of SSI but also reveals a practical need for systems that combine standards compliance, encrypted storage, verifiable credentials, and humane recovery workflows in one deployable architecture.

III. TECHNOLOGY TABLE

Table no. 3.1) Technology Table

Term	Definition	Usage in Project
Ethereum	A decentralized blockchain platform that executes smart contracts and records immutable transactions.	Anchors identity ownership, credential status, issuer registration, and recovery events.
Solidity	A contract-oriented programming language for Ethereum virtual machine applications.	Implements Identity, Credential Registry, Request, and Social Recovery contracts.
IPFS	A peer-to-peer content-addressed storage protocol based on content identifiers (CIDs).	Stores encrypted profile documents and credential payloads off-chain.
React.js / Vite	A frontend library and build environment for responsive single-page web applications.	Provides wallet-connected user interface for profile creation, credential flows, and recovery actions.
Ethers.js / Web3Modal	Libraries used for Ethereum wallet interaction, transaction signing, and provider abstraction.	Connects browser wallets such as MetaMask and signs on-chain operations.
AES-GCM	An authenticated encryption mode that provides confidentiality and integrity protection.	Encrypts sensitive identity data locally before IPFS upload.
W3C Verifiable Credentials	A standards-based model for digitally signed, machine-verifiable claims.	Represents trusted credentials issued by institutions to users and checked by verifiers.
Hardhat	A development environment for compiling, testing, and deploying Solidity contracts.	Used to compile contracts, run local testing, and deploy to the Sepolia test network.

Existing Method: Conventional digital identity solutions rely on centralized databases and third-party identity providers. Even many blockchain-based prototypes stop at immutable registration and do not sufficiently integrate encrypted storage, verifiable credential lifecycles, or resilient account recovery. Common limitations include:

- Lack of privacy-preserving storage for detailed profile attributes.
- Weak key-management and recovery support for ordinary users.
- Limited integration between credential issuance, verification, and revocation.
- Dependence on institution-specific systems that reduce portability and user control.

Comparison Table: Traditional Identity Systems vs. Existing SSI Frameworks vs. DecentraID

Table no. 3.2) Comparison Table

Aspect	Traditional Systems	Existing SSI Tools	DecentraID
Identity ownership	Controlled by service provider or authority.	Usually user-centric, but sometimes tied to specific wallets or ecosystems.	User-controlled identity references with on-chain ownership and off-chain encrypted records.
Privacy	Personal data often stored in plaintext or centrally managed repositories.	Improved privacy, but metadata exposure and storage design vary.	Client-side AES-GCM encryption with minimal on-chain disclosure.
Credential handling	Manual verification or institution-specific portals.	Supported in some frameworks; portability varies.	Credential request, issuance, verification, and revocation linked to on-chain registry.
Recovery	Password reset through centralized administrator.	Often weak or wallet-dependent.	Guardian-based social recovery with threshold approval and time delay.
Interoperability	Low; identity data remains siloed across platforms.	Moderate; depends on DID method and wallet ecosystem.	Designed around W3C-aligned credentials and portable CID-based records.
Trust model	Institutional trust with single point of failure.	Distributed trust, but sometimes complex for end users.	Hybrid trust through blockchain integrity, issuers, and recoverable ownership.

IV. METHODOLOGY

The proposed system follows a layered architecture that separates user interaction, cryptographic protection, decentralized storage, and blockchain-governed trust. This modular design improves maintainability and ensures that privacy-sensitive operations happen on the client side before data leaves the user's device.

1) Client Interface: React-based modules handle wallet connection, profile registration, credential requests, issuer actions, and recovery configuration.
2) Encryption Layer: Before storage, profile and credential payloads are transformed into ciphertext using AES-GCM with keys derived from wallet-assisted signing.
3) Storage Layer: Encrypted content is uploaded to IPFS and identified by content identifiers; only the CID is later referenced on-chain.
4) Blockchain Layer: Ethereum smart contracts maintain identity ownership, issuer permissions, credential status, and social recovery logic.
5) Verification Layer: Authorized verifiers inspect credential metadata, validate signatures, and check revocation status without requesting raw private data from a central server.

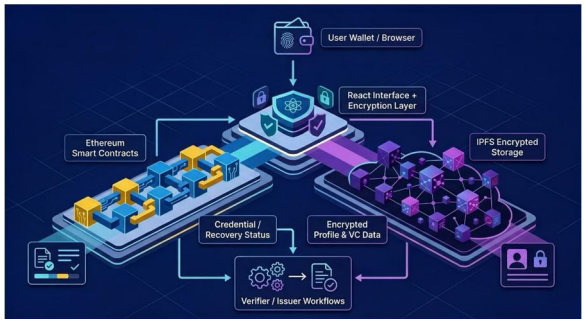
A. Implementation

1) Identity creation: the user enters profile details, encrypts them locally, uploads the encrypted object to IPFS, and stores the returned CID on the Identity smart contract.
2) Credential workflow: the user requests a credential from a trusted issuer; after validation, the issuer uploads the signed credential to IPFS and records metadata plus status on-chain.
3) Identity retrieval: when the holder opens the profile, the application fetches the encrypted IPFS object, re-derives the symmetric key, and decrypts the data in the browser.
4) Revocation and verification: verifiers examine registry metadata and signature information to ensure a credential is genuine, active, and associated with the intended subject.
5) Social recovery: the user appoints guardians and a threshold; if wallet access is lost, guardians approve a new owner address and execute ownership transfer after the configured delay.

B. Technologies Used:

1) Frontend: React.js, Vite, Tailwind CSS
2) Blockchain: Ethereum Sepolia, Solidity, Hardhat
3) Wallet Integration: Ethers.js, Web3Modal, MetaMask
4) Storage: IPFS with Pinata
5) Cryptography: AES-GCM via Web Crypto API
6) Credential Model: W3C DID/VC-aligned JSON structures

Figure no. 4.1) Block Diagram



V. RESULTS AND DISCUSSION

The DecentraID prototype was functionally validated through an end-to-end workflow on Ethereum Sepolia using browser wallets and IPFS-backed storage. As reflected in Figures no. 5.1 to 5.7, the implemented system successfully supported profile creation, encrypted profile updates, credential request and issuance, verification through on-chain status lookup, revocation-aware handling, and guardian-based recovery. These outcomes confirm that the architecture is technically feasible without exposing sensitive user information directly on-chain.

A notable result of the implementation is the practical separation of confidentiality and verifiability. Identity data remain encrypted within IPFS objects, while integrity and status are managed by smart contracts. This design reduces blockchain storage overhead and avoids placing private profile fields on a public ledger. It also improves traceability because credential lifecycle events can be audited through contract state rather than through institutional databases alone [5], [7]. The operational flow illustrated in the dashboard, issuance, and recovery screens further shows that decentralized identity functions can be delivered through a usable web-based interface rather than only as a conceptual protocol.

The social recovery module also addresses a real usability problem in decentralized systems. In many wallet-driven applications, loss of a private key results in permanent identity loss. By introducing guardian approval and delayed execution, DecentraID improves recoverability without reintroducing a centralized administrator. This is especially relevant for student credentials, long-lived professional records, and citizen-facing identity services where key loss cannot be treated as an acceptable risk [8]. The social recovery screen in Figure no. 5.7 demonstrates that the recovery model is not merely theoretical, but integrated into the operational prototype.

At the same time, the implementation reveals several practical challenges. Gas fees, even on a low-cost or test network, remain a consideration for frequent on-chain updates. Credential interoperability also depends on consistent issuer behavior and standards-compliant payload construction. In addition, although AES-GCM protects data confidentiality, future systems should move toward selective disclosure and zero-knowledge proofs so that verifiers can confirm claims without requesting full credential contents [7], [12], [13]. The present study focused on functional validation rather than benchmark-scale performance testing, so metrics such as gas-cost distribution, transaction latency, and encryption overhead should be treated as important next-step evaluation targets rather than as claims established here.

Overall, the results suggest that DecentraID offers a more privacy-aware and user-controlled alternative to traditional identity systems while remaining implementable with widely available Web3 tooling. The prototype does not claim to solve all SSI challenges, but it demonstrates a coherent and deployable combination of blockchain integrity, decentralized storage, standards-based credentials, and recoverable identity ownership. From a publication standpoint, the strongest contribution of the work lies in integrating encrypted off-chain storage, credential lifecycle support, and social recovery into a single end-to-end academic prototype.

A. Functional Validation Summary

1) Home Page: The landing page serves as the main entry point of DecentraID and introduces the platform's self-sovereign identity concept before any blockchain interaction begins.

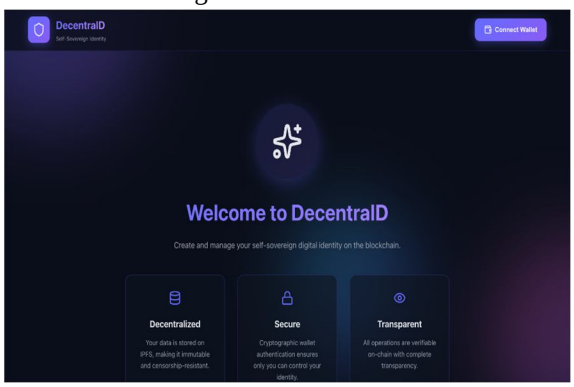


Figure no. 5.1) Homepage

2) Wallet Connection Dialog: This screen shows the MetaMask authorization step where the user selects an account and grants permission to connect the wallet with the decentralized application.

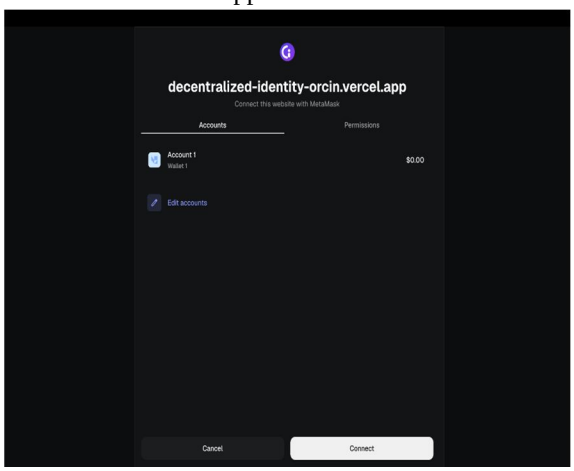


Figure no. 5.2) Wallet Connection Dialog

3) Identity Creation and Signature Request: When the connected account has no registered identity, the system prompts the user to create one. The signature request is used in the protected client-side encryption flow before profile data is stored.

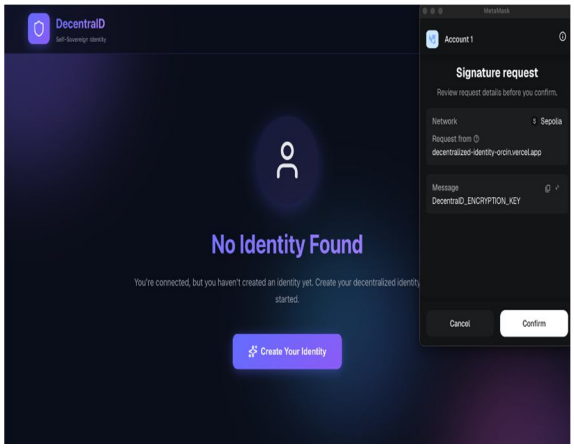


Figure no. 5.3) Identity Creation and Signature Request

4) Identity Update / Document Upload: This interface captures government and identity-document details such as document type, identifier, and supporting file upload, representing the secure profile enrichment stage of the identity workflow.

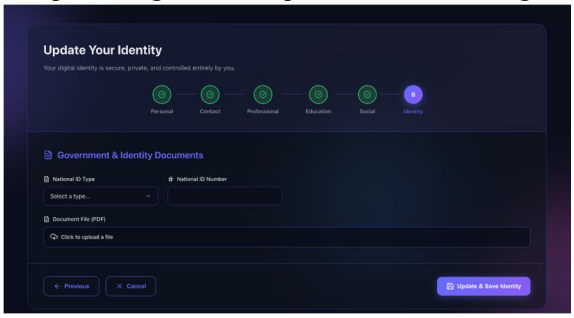


Figure no. 5.4) Identity Update / Document Upload

5) Profile Dashboard: The profile dashboard confirms successful identity creation by displaying personal information, contact data, blockchain-linked identifiers, DID references, and profile metadata retrieved through the application.

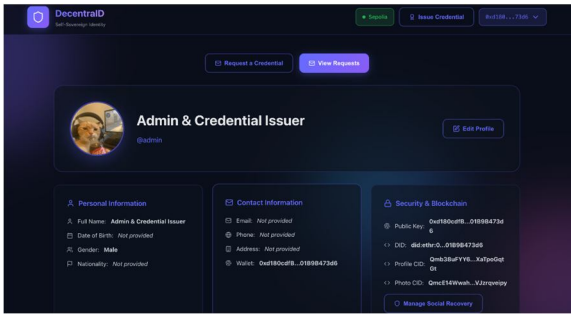


Figure no. 5.5) Profile Dashboard

6) Credential Issuance Form: This issuer-facing screen demonstrates how an authorized issuer can create a new verifiable credential by specifying the subject address, credential type, description, and optional expiry information.

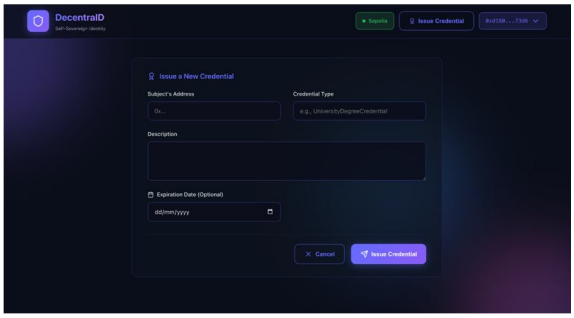


Figure no. 5.6) Credential Issuance Form

7) Social Recovery Management: The guardian-management interface represents the social recovery component of DecentraID, where trusted guardian addresses can be configured and recovery status can be monitored for resilient account restoration.

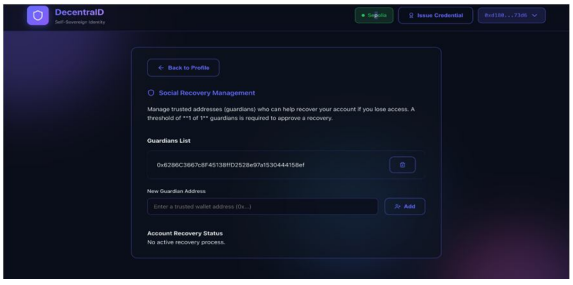


Figure no. 5.7) Social Recovery Management

Table no. 5.1 Function Validation

Scenario	Expected Outcome	Observation
Identity registration	Encrypted profile stored on IPFS and CID linked on-chain.	Successfully completed with wallet-signed transaction and retrievable CID.
Credential issuance	Issuer records a verifiable credential reference and status.	Credential metadata stored and available for later verification.
Credential revocation	Registry marks credential invalid without deleting record.	Revocation status remained auditable through smart contract state.
Profile retrieval	Only holder can decrypt stored profile data.	Decryption succeeded locally after wallet-assisted key derivation.
Social recovery	Guardians approve transfer of ownership after threshold and delay.	Recovery flow executed correctly in functional tests.

VI. FUTURE SCOPE

1) Conduct systematic performance evaluation, including gas consumption, transaction latency, IPFS retrieval delay, and encryption/decryption overhead, to complement the present functional validation.

2) Integrate selective disclosure and zero-knowledge proof mechanisms for privacy-preserving attribute verification without revealing full credential contents.

3) Extend support to additional blockchain networks such as Polygon or Arbitrum to reduce transaction cost and improve deployment flexibility.

4) Strengthen standards compliance through richer DID resolution support, broader VC interoperability testing, and issuer-verifier compatibility checks.

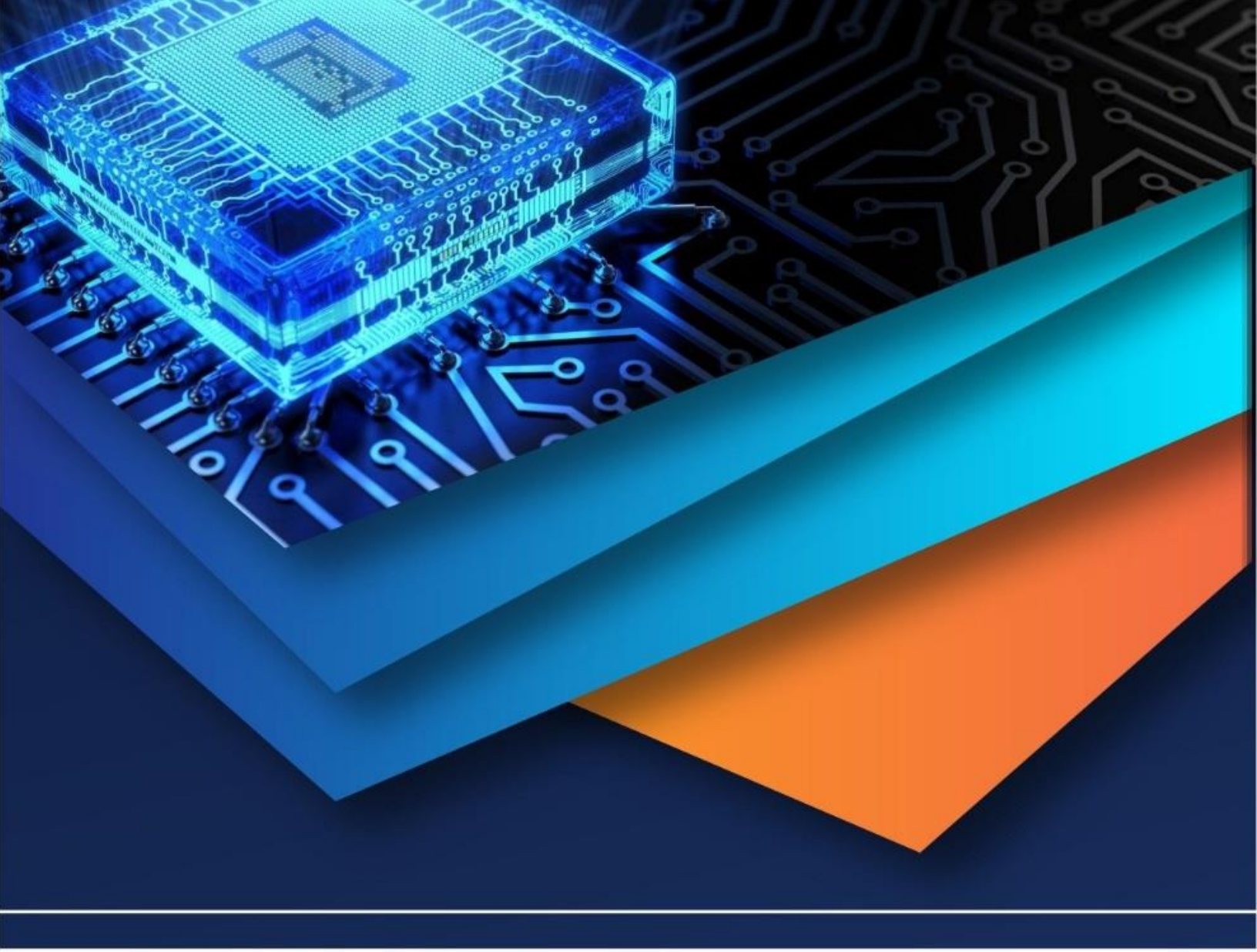
5) Add mobile-wallet support and governance features, including issuer onboarding policies, institutional trust frameworks, and production-grade recovery safeguards.

VII. CONCLUSION

This paper presented DecentraID, a blockchain-based self-sovereign identity system designed to improve privacy, portability, and user control in digital identity management. By combining Ethereum smart contracts with IPFS-backed encrypted storage, the framework separates public verifiability from private data confidentiality. Its support for W3C-aligned credentials and guardian-based social recovery makes the system more usable than many minimal blockchain identity prototypes. The implementation demonstrates that decentralized identity can move beyond theory when identity ownership, credential workflows, storage efficiency, and recovery are treated as an integrated design problem. For academic and institutional settings in particular, DecentraID offers a practical foundation for secure and portable digital identity.

REFERENCES

[1] A. Giannopoulou, “A Critical Approach of Self-Sovereign Identity,” Digital Society, vol. 2, no. 3, 2023. doi: 10.1007/s44206-023-00049-z.
[2] R. Dutra Garcia, G. Ramachandran, K. Dunnett, R. Jurdak, C. Ranieri, B. Krishnamachari, and J. Ueyama, “A Survey of Blockchain-Based Privacy Applications: An Analysis of Consent Management and Self-Sovereign Identity Approaches,” arXiv:2411.16404, 2024.
[3] W3C, “Decentralized Identifiers (DIDs) v1.0,” W3C Recommendation, Jul. 19, 2022.
[4] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, M. Conti, “A Survey on Decentralized Identifiers and Verifiable Credentials,” arXiv:2402.02455, 2024.
[5] IPFS Docs, “What is IPFS?” and “Content Identifiers (CIDs),” Protocol Labs Documentation, accessed Mar. 2026.
[6] J. Benet, “IPFS – Content Addressed, Versioned, P2P File System,” arXiv:1407.3561, 2014.
[7] W3C, “Verifiable Credentials Data Model v2.0,” W3C Recommendation, May 15, 2025.
[8] J. Zhang, D. Xiang, K. Xu, and G. Zhang, “ERC-7093: Social Recovery Interface,” Ethereum Improvement Proposal, May 2023.
[9] R. A. Pava-Diaz, J. Gil-Ruiz, and D. A. Restrepo, “Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation,” Frontiers in Blockchain, 2024. doi: 10.3389/fbloc.2024.1443362.
[10] W. Chan, “Blockchain-Assisted Self-Sovereign Identities on Education: Opportunities and Challenges,” Blockchains, vol. 3, no. 1, 2025. doi: 10.3390/blockchains3010003.
[11] Y.-H. Hsieh, Y.-H. Hsiao, and C.-M. Chen, “Self-Sovereign Identity-Based E-Portfolio Ecosystem,” Applied Sciences, vol. 14, no. 22, 2024. doi: 10.3390/app142210361.
[12] D. Naicker, M. Gerber, and E. van der Poll, “Challenges of user data privacy in self-sovereign identity implementations,” Frontiers in Blockchain, 2024. doi: 10.3389/fbloc.2024.1374655.
[13] J. He, X. Wei, and X. Liu, “Supervised and revocable decentralized identity privacy protection based on blockchain,” Security and Safety, 2024.
[14] NIST, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC,” SP 800-38D; revision notice, Mar. 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY