WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Empowering Self-Sovereign Digital Identities: A Blockchain and AI-Driven Approach for Enhanced Privacy and Security

[1]Angelin Rosy M, [2]Indhumathi J

[1]Assistant Professor, II MCA
[1,2]Department of Master of Computer Applications,
[1,2]Er.Perumal Manimekalai College of Engineering, Hosur,
[1]angelinrosym@gmail.com, [2]hindhuindhu8@gmail.com

DOI : https://doi.org/10.5281/zenodo.15597854

ABSTRACT:

With the rapid rise in digital services, managing personal identity online has become both essential and challenging. Most current systems rely on centralized or federated identity models, which often compromise user privacy and are vulnerable to data breaches. Centralized systems store user data in a single location, increasing the risk of large-scale attacks, while federated models allow third-party providers to access and track user information without clear consent. To address these concerns, this paper introduces a Self-Sovereign Identity (SSI) solution that gives users full control over their digital identity. The proposed system, called Sign Up Wallet, leverages blockchain technology for secure, decentralized identity storage and uses cryptographic methods to protect user credentials. To ensure trust, the system integrates a machine learning model—Logistic Regression—to evaluate whether a service provider is reliable. If a provider is flagged as untrusted, the system generates a masked version of the user's identity using a Lookup Substitution Algorithm, allowing safe verification without exposing actual data. This approach significantly enhances privacy, security, and user autonomy, reducing reliance on centralized authorities and offering a more transparent and trustworthy identity framework.

Keywords: Digital identity, blockchain, self-sovereign identity, artificial intelligence, privacy, decentralized system, logistic regression.

INTRODUCTION

As more of our daily activities move online—whether it's checking our bank balance, signing up for government services, or applying for a new job—our digital identity becomes a key part of how we interact with the world. But even though we rely on it so much, the way digital identity is handled today often puts users at risk and gives them very little control.

Most online identity systems follow one of two approaches: centralized or federated. In centralized systems, all your personal details are stored in a single location, such as a government or company server. If that one system is compromised, all your data is suddenly exposed. Federated systems, like signing in with Google or Facebook, may be more convenient, but they come with a tradeoff—these platforms can track your activity across services, often without your knowledge or full consent.

In both cases, the real problem remains: you're not the one in control of your identity. Someone else is managing it, storing it, and deciding how it's used.

That's why there's growing interest in a new approach called Self-Sovereign Identity (SSI). "With SSI, you're the one in charge—you build your own digital identity, keep your credentials safe, and decide exactly what to share, and when."

This paper introduces Sign Up Wallet, a modern identity system built on the SSI concept. It combines blockchain for secure and decentralized storage, cryptography for protecting user credentials, and artificial intelligence to check whether a service requesting your identity can be trusted. If the system detects risk, it can mask your sensitive information while still letting you verify your eligibility. With Sign Up Wallet, users finally get the power to manage their identities safely, privately, and on their own terms.

RELATED WORK

- In recent years, digital identity has seen major improvements, particularly through blockchain technology. Several projects like uPort, Sovrin, and Civic have developed decentralized identity platforms that empower users to own and manage their personal data. These systems introduced important ideas such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), moving away from the old model where user data is stored in a single centralized location.
- However, a common shortcoming of these platforms is that they focus mostly on how identity data is stored and shared, without checking whether the service requesting the data is trustworthy. They don't provide mechanisms to evaluate the safety or reliability of the entities asking for your information.

- In contrast, some other sectors like online shopping have started using artificial intelligence to determine the trustworthiness of sellers or service providers, based on reviews, ratings, or complaint records. But integrating AI-based trust evaluation directly into identity management systems is still quite rare.
- The Sign Up Wallet system addresses this gap. It not only offers secure, decentralized identity storage but also uses machine learning to assess whether the service requesting your identity can be trusted. If the service appears risky, the system protects your real data by sharing a masked version instead, significantly boosting user privacy and security.

PROPOSED WORK

The proposed system is designed to give users full control over their digital identities using blockchain and artificial intelligence. Instead of relying on centralized servers, the system allows users to create their own decentralized identity (DID), which is stored securely on a blockchain. Once a user registers and verifies their email, the system issues digital credentials that are linked to the user's DID. These credentials are encrypted and stored in a decentralized storage system, while only the hashed reference is saved on the blockchain to ensure privacy. To enhance security, AI algorithms are used to verify users through behavior analysis and detect any unusual activity or fraud. The system includes a user-friendly interface for managing credentials and sharing them with full consent. Overall, the platform ensures privacy, security, and transparency while allowing users to control and protect their identity information.

METHODS

The Sign Up Wallet system is designed by integrating multiple technologies to offer users both control and strong security over their digital identities. It is built around four main components:

A . Blockchain for Decentralized Identity

Instead of saving your identity data in a single centralized database, the Sign Up Wallet records the proofs of your credentials on a blockchain. This distributed ledger is secure and immutable, meaning no single party can alter or delete your information. You retain ownership of your identity by holding private cryptographic keys, while the blockchain guarantees the integrity and authenticity of your data.

B. Identity Wallet (User Interface)

Users interact with their digital identity through an intuitive app called Sign Up Wallet. This wallet securely stores your credentials—such as your age, citizenship, or educational background—right on your device in encrypted form. When a service requests information, you choose exactly what to share. For example, you can confirm you are over 18 without revealing your full birthdate.
The wallet also lets you easily accept or decline any requests for your personal data, putting you in full control of your identity.

C. *AI-Based Trust Evaluation*

Before sharing any identity information, the system runs a trust check on the requesting service provider. Using a Logistic Regression machine learning model, it assesses trustworthiness by analyzing factors like past complaints, response times, and previous behavior patterns.
If the provider passes the trust threshold, your real identity details are shared. If not, the system employs protective measures to mask your information, safeguarding your privacy.

Step-by-Step Process:

- User Account Creation :The user begins by registering on the platform and submitting essential information such as their email address and identification details.
- Email Verification :A unique verification link is generated and sent to the user's email. Upon clicking the link, the user's identity is confirmed, enabling further system access.
- Decentralized Identifier (DID) Generation:After successful verification, the system creates a unique DID for the user, representing their self-owned digital identity on a decentralized network.
- Verifiable Credential (VC) Issuance:Digital credentials linked to the DID are issued, encrypted, and stored using decentralized storage like IPFS, ensuring both privacy and authenticity.
- Blockchain Anchoring:Hashed records of the credentials and identity actions are stored on the blockchain, providing immutability, traceability, and tamper resistance.
- AI-Based Identity Verification:Machine learning models assess user behavior and credentials to detect anomalies, assign trust scores, and strengthen fraud prevention.

Secure and Private Access:Once all verifications are complete, users can securely manage and share their digital identities with full control, ensuring data privacy and system integrity.

MODULES:

A. ***User Registration and Email Verification Module:***

This module facilitates user onboarding by collecting essential information, including the email address, during registration. After receiving the user's registration details, the system generates a unique verification code and sends it to the registered email address. When the user accesses the provided link, the system validates the token against its records. If the token is valid and active, the user is authenticated and granted access, ensuring that only verified individuals can interact with the platform.

B. Decentralized Identity Management Module:

After verification, a Decentralized Identifier (DID) is created for the user. This DID serves as a globally unique identifier, independent of any centralized registry. The system follows W3C DID standards to ensure compatibility and interoperability. This module handles the creation, updating, and deactivation of DIDs securely.

C. Verifiable Credential Issuance Module:

This module facilitates the issuance of digital credentials, such as ID proofs or academic certificates, by trusted issuers. These credentials are cryptographically signed and linked to the user's DID. The credentials are stored in encrypted form using decentralized storage solutions like IPFS, while only their hashes are stored on the blockchain to ensure tamper-resistance.

D. Blockchain Integration Module:

The blockchain module is responsible for storing hashed references to the verifiable credentials and maintaining a tamper-proof record of identity-related actions. Smart contracts handle the secure recording of credential generation, cancellation, and validation operations on the blockchain.This ensures transparency, traceability, and integrity of identity data.

E. AI-Based Identity Verification Module:

This module employs machine learning techniques to strengthen the identity verification process and identify suspicious or fraudulent activities.. AI models are trained to analyze login patterns, behavioral biometrics, and device usage. Based on these factors, a trust score is generated, helping the system to make intelligent decisions about access control and anomaly detection.

F. Credential Sharing and Access Control Module:

Users can share their verifiable credentials with third-party verifiers through this module. Each sharing action requires user consent and is traceable. Access control policies ensure that only authorized entities can view the shared data, preserving user privacy and control.

G. User Interface Module:

This module provides a simple and intuitive interface for users to register, verify, manage credentials, and monitor activity logs. It serves as a bridge between users and the backend system, ensuring a smooth and secure user experience across web and mobile platforms.

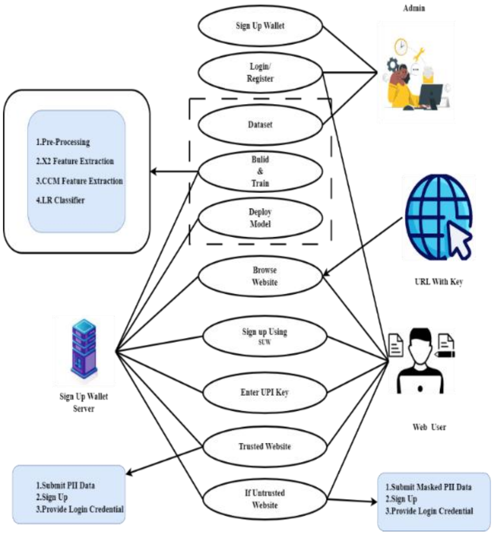


Figure 1:System architecture

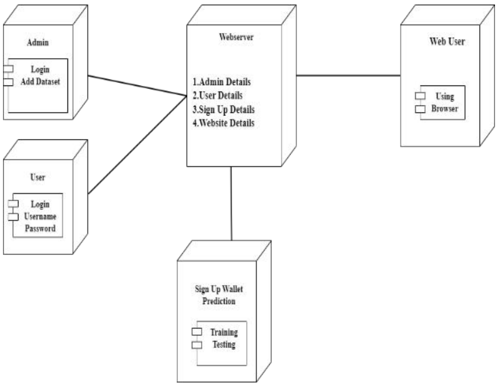
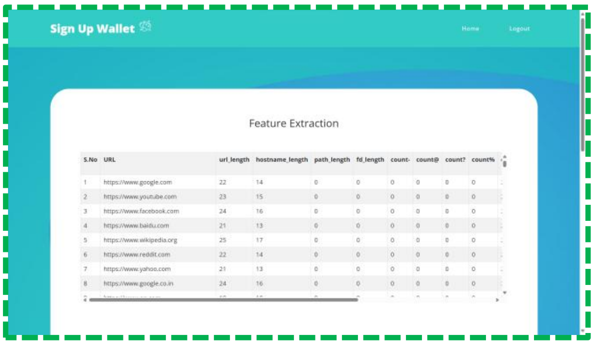


Figure 2:Divid architecture

RESULTS

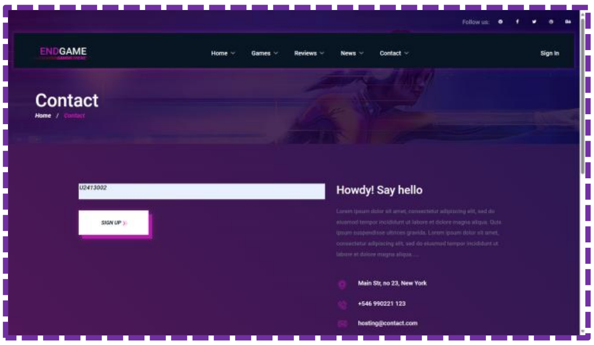
The proposed system fosters a more secure, private, and user-centric approach to digital interactions, marking a significant step towards a future where individuals truly own and govern their online presence.

- **Empowers Users:** This system grants individuals full control over their digital identity, enhancing privacy and security.
- **Decentralized Trust:** It replaces vulnerable centralized systems with a blockchain-based, ML-enhanced approach for more secure and private online interactions.



Feature Extraction

S.No	URL	url_length	hostname_length	path_length	fd_length	count-	count@	count?	count%
1	https://www.google.com	22	14	0	0	0	0	0	0
2	https://www.youtube.com	23	15	0	0	0	0	0	0
3	https://www.facebook.com	24	16	0	0	0	0	0	0
4	https://www.baidu.com	21	13	0	0	0	0	0	0
5	https://www.wikipedia.org	25	17	0	0	0	0	0	0
6	https://www.reddit.com	22	14	0	0	0	0	0	0
7	https://www.yahoo.com	21	13	0	0	0	0	0	0
8	https://www.google.co.in	24	16	0	0	0	0	0	0



U2413002

Howdy! Say hello

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. ...

Main Str, no 23, New York
+546 990221 123
hosting@contact.com

CONCLUSION

This project establishes an advanced method to combat phishing threats by using Visual Cryptography with One-Time Password (OTP) technology. The system protects data authenticity and user identification through secure OTP development together with image improvement steps coupled with dual verification procedures.

The system uses visual cryptography mechanics that split user-based images into shares alongside time-sensitive OTPs to minimize unauthorized access attempts. The preprocessing procedures simultaneously boost system accuracy while protecting against conventional phishing attempts which makes the model appropriate for real-world deployment while ensuring security.

The developed authentication framework offers a resilient solution against phishing threats while appropriately addressing end-user needs for easy operation.

Conflict of Interest:The authors have verified that this study lacks any conflicting interests.

Funding Disclosure: There was no financial support or third-party funding used for performing this research project.

Ethical Approval: The researchers performed this study devoid of experiments which included human or animal participants.
Consent Disclosure: The study omitted patient-related data so consent procedures were not required.

ACKNOWLEDGMENT

The authors declare that they have no reports of acknowledgments for this

REFERENCES:

1. M. S. Ferdous, A. Ionita and W. Prinz, "SSI4Web: A self-sovereign identity (SSI) framework for the web", Proc. Int. Congr. Blockchain Appl., pp. 366-379, 2023.
2. Y. Bai, H. Lei, S. Li, H. Gao, J. Li and L. Li, "Decentralized and self-sovereign identity in the era of blockchain: A survey", Proc. IEEE Int. Conf. Blockchain (Blockchain), pp. 500-507, Aug. 2022.
3. K. P. Jørgensen and R. Beck, "Universal wallets", Bus. Inf. Syst. Eng., vol. 64, no. 1, pp. 115-125, Feb. 2022.
4. Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović and M. Turkanović, "Towards the classification of self-sovereign identity properties", IEEE Access, vol. 10, pp. 88306-88329, 2022.
5. B. Podgorelec, L. Alber and T. Zefferer, "What is a (Digital) identity wallet? A systematic literature review", Proc. IEEE 46th Annu. Comput. Softw. Appl. Conf. (COMPSAC), pp. 809-818, Jun. 2022.
6. S. Schwalm, D. Albrecht and I. Alamillo, "eIDAS 2.0: Challenges perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI" in Open Identity Summit, Bonn, Germany:Gesellschaft für Informatik, pp. 63-74, 2022.
7. W. Fdhila, N. Stifter, K. Kostal, C. Saglam and M. Sabadello, "Methods for decentralized identities: Evaluation and insights", Proc. Int. Conf. Bus. Process Manage., pp. 119-135, 2021.
8. J. Sedlmeir, R. Smethurst, A. Rieger and G. Fridgen, "Digital identities and verifiable credentials", Bus. Inf. Syst. Eng., vol. 63, no. 5, pp. 603-613, Oct. 2021.
9. H. Yildiz, C. Ritter, L. T. Nguyen, B. Frech, M. M. Martinez and A. Küpper, "Connecting self-sovereign identity with federated and user-centric identities via SAML integration", Proc. IEEE Symp. Comput. Commun. (ISCC), pp. 1-7, Sep. 2021.
10. A.Grüner, A. Mühle and C. Meinel, "Analyzing interoperability and portability concepts for self-sovereign identity", Proc. IEEE 20th Int. Conf. Trust Secur. Privacy Comput. Commun. (TrustCom), pp. 587-597, Oct. 2021.