International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

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

**Mrs. M.Hemalatha,Sriram R.K, Sabari P , Ramis raj L, Sugumaran M**

*Computer science and Engineering & Dhanalakshmi Srinivasan Engineering College*
*Computer science and Engineering & Dhanalakshmi Srinivasan Engineering College*
*Computer science and Engineering & Dhanalakshmi Srinivasan Engineering College*

---

**Abstract -** The project aims to revolutionize digital identity management by introducing a secure, decentralized, and user-centric approach. It addresses the limitations of existing centralized and federated systems, empowering individuals with greater control over their digital identities while enhancing security and privacy.To achieve this, the project will create an advanced Self-Sovereign Identity (SSI) model using blockchain and machine learning. Blockchain will be utilized for secure and tamper-resistant storage of digital identities, and Logistic Regression will be incorporated to predict service provider trustworthiness. The system, named Self Sovereign Vault, is designed for user-controlled digital identity and will establish a Unique Personal Identifier (UPI) Code system for streamlined authentication.Additionally, a Lookup Substitution Algorithm will generate masked credentials in untrusted scenarios, enhancing data portability across platforms and reducing reliance on centralized authorities. Advanced security measures will be implemented to mitigate the risks of large-scale hacks and data breaches.

***Key Words*:** Self-Sovereign Identity, Blockchain, Logistic Regression, Digital Identity, Privacy

## 1.INTRODUCTION

The introduction of the document explains that signing up refers to creating an online account using an email address or username and password for a website or web-based service. After signing up, users can access their accounts by logging in. A signup form is a web page, popup, or modal where users enter the necessary information to access the website's services. The information collected depends on the website and its services, but most forms require a name, email address, username, and password

## 2. OBJECTIVE

To Develop a Robust Self-Sovereign Identity (SSI) Model: Create an advanced SSI model using blockchain and machine learning.

To Implement Tamper-Resistant Blockchain Storage: Utilize blockchain for secure and tamper-resistant storage of digital identities.

To Integrate Logistic Regression for Trust Prediction: Incorporate Logistic Regression to predict service provider trustworthiness.

To Enable User-Centric Identity Management: Design Self Sovereign Vault for user-controlled digital identity.

To Establish a Unique Personal Identifier (UPI) Code System: Develop a UPI Code system for streamlined authentication.

To Implement a Lookup Substitution Algorithm: Create an algorithm for generating masked credentials in untrusted scenarios.

To Enhance Data Portability Across Platforms: Ensure seamless management of digital identities across various services.

## 3.EXISTING SYSTEM

The existing digital identity management systems rely on centralized and federated approaches, which face challenges compromising user privacy and security. Centralized systems are prone to large-scale hacks and breaches, putting user data at substantial risk. Federated models enable companies to track user data without explicit consent, raising privacy concerns. Traditional systems lack portability of identity data and fail to empower individuals with control over their digital identities

### 3.1DISADVANTAGES

Lengthy and complex registration forms can lead to user frustration and abandonment of the sign-up process.

Users often struggle with managing multiple passwords for various online accounts, which can lead to forgetfulness, password reset requests, and increased security breach risks.

Relying on email verification for user confirmation can cause delays due to spam filters or delivery issues, negatively impacting the user experience

## 4.PROPOSED SYSTEM

The Self-Sovereign Vault system is designed to provide users with a secure and user-centric platform for digital identity management. The core of this system is the WalletChain, a digital wallet enhanced by blockchain technology, which securely stores users' Personal Identifiable Information (PII). Users interact with the system through the Self-Sovereign Vault Web App, where they can store their digital identities in the WalletChain. The system uses a Unique Personal

Identifier (UPI) Code for each user and incorporates multi-step verification during registration.

### 4.1ADVANTAGES

**Greater control over digital identities:** The system empowers individuals with increased control over their digital identities.

**Reduced reliance on centralized entities:** It minimizes dependence on centralized authorities for identity verification.

**Enhanced security:** The system incorporates advanced security measures to mitigate the risks of large-scale hacks and data breaches.

**Improved privacy:** The system preserves user privacy through features like masked credentials and decentralized storage

## 5.SYSTEM ARCHITECTURE

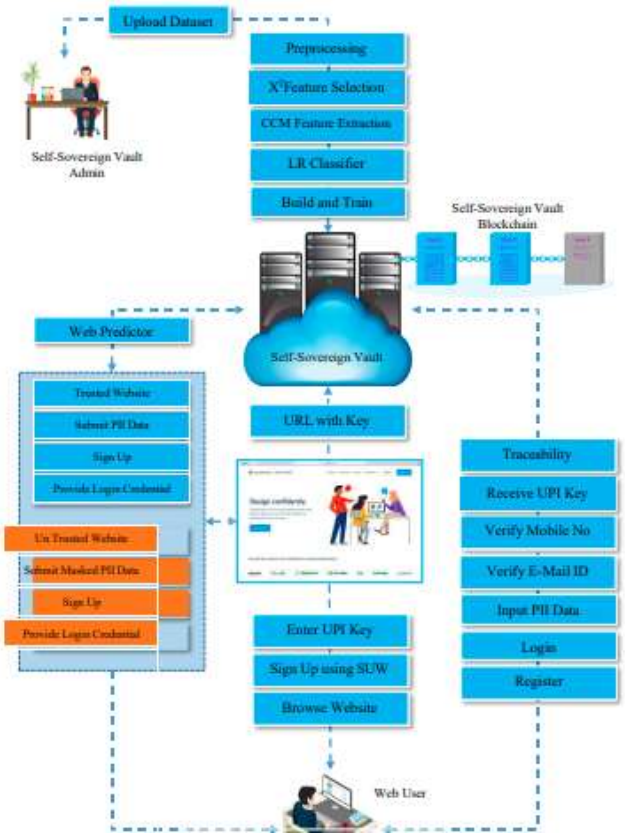


**Fig (System Architecture)**

## 6.METHODOLOGY

### SYSTEM DESIGN AND ARCHITECTURE

The system architecture integrates blockchain for secure identity storage and management, utilizing a Self-Sovereign Identity model. Logistic Regression aids in predicting website trustworthiness. The system uses a Unique Personal Identifier (UPI) Code for user registration. A Lookup Substitution Algorithm generates masked credentials.

### WALLET CHAIN INTEGRATION

Self-Sovereign Vault system introduces the concept of a WalletChain, which is a digital wallet fortified by blockchain technology. The WalletChain serves as a secure repository for users to store their Personal Identifiable Information (PII), personal attributes, and other relevant data. Users can store their digital identity within the WalletChain using the Self-Sovereign Vault Web App. Blockchain technology ensures the immutability and tamper-resistant nature of this stored data.

### USER INTERFACE DESIGN

The Self-Sovereign Vault web application is developed using Python, Flask, MySQL, and Bootstrap. The User Registration Module allows account creation with a Unique Personal Identifier (UPI). The Login Module provides secure access. The Dashboard Module gives users an overview of linked services and credentials. Users can manage their information through the Digital Identity Management Module. The Wallet Module handles cryptographic keys and transactions

### TESTING AND VALIDATION

System validation followed a multi-phase approach:

1. It includes various types of testing, including load testing, stress testing, endurance testing, scalability testing, volume testing, usability testing, and compatibility testing.
2. It includes a section on test cases, providing specific examples such as admin login, model training, user management, and system maintenance.
3. For each test case, the document outlines the input, expected result, actual result, and status (pass/fail).
4. The testing and validation process aims to ensure the system's functionality, performance, and reliability across different scenarios and platforms

### PERFORMANCE EVALUATION

We evaluated system performance using quantitative metrics including:

- Face recognition accuracy (precision, recall, F1-score)
- System response time for attendance marking
- Notification delivery success rate and latency
- Administrative time savings compared to manual methods

## 7.CONCLUSIONS

The project aims to revolutionize digital identity management by introducing a secure, decentralized, and user-centric approach. It addresses the limitations of existing centralized and federated systems, empowering individuals with greater control over their digital identities while enhancing security and privacy. By combining blockchain for self-sovereign identity management and machine learning for predicting trusted websites, the Self Sovereign Vault project seeks to offer individuals greater control, reduce reliance on centralized entities, and mitigate risks associated with data breaches and privacy violations.

## 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. 89
11. N. Naik and P. Jenkins, "Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology", Proc. IEEE Int. Symp. Syst. Eng. (ISSE), pp. 1-7, Sep. 2021.
12. A.Giannopoulou, "Data protection compliance challenges for self-sovereign identity", Proc. 2nd Int. Congr. Blockchain Appl., pp. 91-100, 2020.
13. Z. A. Lux, D. Thatmann, S. Zickau and F. Beierle, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials", Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS), pp. 71-78, Sep. 2020.
14. C. Shaik, "Securing cryptocurrency wallet seed phrase digitally with blind key encryption", Int. J. Cryptogr. Inf. Secur., vol. 10, no. 4, pp. 1-10, Dec. 2020.
15. Grüner, A. Mühle and C. Meinel, "An integration architecture to enable service providers for self-sovereign identity", Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA), pp. 1-5, Sep. 2019.