International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

SIGN UP WALLET USING BLOCKCHAIN TECHNOLOGY

P.Rithanya
Electronics and communication Engineering
Bannari Amman Institute Of technology
Sathyamangalan,India

A.L.Thirukkural Selvan
Computer Science and Engineering
Bannari Amman Institute Of technology
Sathyamangalan,India

V.Sowmiya
Electronics and communication Engineering
Bannari Amman Institute Of technology
Sathyamangalan,India

Mr S Suseendran
Professor
Computer Science and Engineering
Bannari Amman Institute Of technology
Sathyamangalan,India

***Abstract*— Digital identity serves as an individual's online identification, akin to physical documents like passports or driver's licenses. It encompasses unique characteristics or attributes specific to each person. In the digital realm, organizations typically rely on centralized or federated identity management systems. However, centralized systems pose risks by making user data susceptible to large-scale breaches. Conversely, federated models enable data tracking by companies. Current identity management systems often center around centralized authentication servers, proving inadequate in safeguarding user privacy and facilitating seamless identity data portability. A dependable system is necessary for secure digital interactions. These challenges led to the development of Sign-Up Wallet, a blockchain and machine learning-based solution for managing digital identities. Blockchain technology enables self-sovereign identity management, eliminating the need for trusted third parties. Machine learning aids in identifying trusted service providers. In this proposed system, users store their digital identities in Sign-Up Wallet with cryptographic keys. When registering with a trusted service provider, a Unique Personal Identifier (UPI) Code is used for direct credential verification. Logistic Regression helps predict the trustworthiness of websites. If a service provider is deemed untrustworthy, a masked credential is generated, preserving privacy during verification. This masked credential is then provided to the service provider, maintaining user security without exposing raw data. The primary aim of this project is to empower individuals with greater control over their digital identities, reducing reliance on centralized authorities and mitigating risks associated with data breaches and privacy violations.**

Keywords—Digital identity, Centralized, Federated, Authentication, Privacy, Blockchain, Self-sovereign identity, Machine learning, Trusted service provider, Privacy-preserving.

I. INTRODUCTION

Lengthy and complex registration forms can result in user frustration and abandonment of the sign-up process. High friction during registration can negatively impact user acquisition and retention. Users often struggle with managing multiple passwords for various online accounts. This can lead to forgetfulness, password reset requests, and an increased risk of security breaches. The common practice of relying on email verification for user confirmation can introduce delays, and users may encounter issues with spam filters or delayed delivery, affecting the overall user experience. SMS or mobile app verification may be inconvenient for users without easy access to mobile devices or those in areas with limited network coverage. Users may be reluctant to provide extensive personal information during the registration process due to privacy concerns. Collecting unnecessary data may hinder user trust and adoption. Once personal information is submitted, users often have limited control over how their data is used. Centralized storage of user information poses a higher risk of data breaches, impacting user privacy. Different platforms may have varying registration processes, creating inconsistencies in user experience and potentially causing confusion for users. Users may hesitate to provide their primary email addresses due to concerns about receiving spam or unwanted promotional emails. Captcha challenges, while introduced for security, can sometimes be difficult for users to complete, leading to frustration. The existing digital identity management systems, relying on centralized and federated approaches, face significant challenges that compromise user privacy and security. Centralized systems, prone to large-scale hacks and breaches, put user data at substantial risk. Meanwhile, federated models enable companies to track user data without explicit consent, raising concerns about data privacy. Moreover, traditional identity management systems lack the portability of identity

data and fail to empower individuals with control over their digital identities. These shortcomings have led to increased cybersecurity spending each year, reflecting the ongoing battle against data breaches and privacy violations. By combining blockchain for self-sovereign identity management and machine learning for predicting trusted websites, the Sign-Up Wallet project seeks to offer individuals greater control over their digital identities, reduce reliance on centralized entities, and mitigate the risks associated with data breaches and privacy violations.

II. Literature Survey

Recent advancements in digital identity and blockchain technologies have led to significant progress in various domains. Ferdous et al. [1] introduced the SSI4Web framework, aiming to establish a robust self-sovereign identity (SSI) system tailored specifically for web environments. This framework holds promise in providing individuals with greater control over their personal data and identity management while ensuring security and privacy. Building upon this foundation, Bai et al. [2] conducted an extensive survey focusing on decentralized and self-sovereign identity systems within the context of blockchain technology. This work serves as a valuable resource for researchers and practitioners alike, guiding future developments and implementations. Jørgensen and Beck [3] explored the concept of universal wallets, which play a crucial role in facilitating secure and convenient management of digital assets. By examining the functionalities and implications of universal wallets, this study contributes to the ongoing discussions surrounding the broader adoption of digital identity solutions. Moving forward, Čučko et al. [4] proposed a classification framework for self-sovereign identity properties, aiming to provide a structured approach for understanding and categorizing various aspects of SSI systems. Podgorelec et al. [5] conducted a systematic literature review on digital identity wallets, shedding light on their diverse functionalities and applications. Schwalm et al. [6] addressed the challenges and proposed solutions for aligning eIDAS regulations with self-sovereign identity systems. Their work emphasizes the importance of regulatory compliance and interoperability in fostering the adoption of SSI frameworks. Additionally, Fdhila et al. [7] evaluated various methods for decentralized identities, providing valuable insights into their effectiveness and suitability for different use cases. By examining the strengths and limitations of these methods, this study offers guidance for organizations seeking to implement decentralized identity solutions. Sedlmeir et al. [8] delved into digital identities and verifiable credentials, emphasizing their role in enhancing security and trust in digital transactions. Their work underscores the importance of robust identity verification mechanisms in safeguarding against identity fraud and unauthorized access. Yildiz et al. [9] explored the integration of self-sovereign identity with federated and user-centric identities via SAML integration. Their study elucidates the potential synergies between different identity management paradigms, paving the way for enhanced interoperability and user experience. Grüner et al. [10] undertook an analysis of interoperability and portability concepts for self-sovereign identity, elucidating the key factors influencing the seamless exchange of digital identities across diverse platforms. Their insights offer valuable guidance for achieving greater flexibility and adaptability in identity management systems. Naik and Jenkins [11] conducted an analysis of the Sovrin network for decentralized digital identity, focusing on its implementation based on distributed ledger technology. Their study provides valuable insights into the technical and practical considerations of deploying decentralized identity solutions at scale. Giannopoulou [12] addressed the data protection compliance challenges associated with self-sovereign identity systems. By highlighting the regulatory and legal implications, their work contributes to a better understanding of the privacy and security considerations inherent in decentralized identity architectures. Lux et al. [13] presented a distributed ledger-based authentication approach leveraging decentralized identifiers and verifiable credentials. Their study explores novel methods for enhancing the security and reliability of digital identity verification processes, particularly in decentralized environments. Shaik [14] proposed a method for securing cryptocurrency wallet seed phrases digitally using blind key encryption techniques. This innovative approach offers enhanced protection for sensitive cryptographic keys, mitigating the risks associated with unauthorized access and theft in cryptocurrency ecosystems. Grüner et al. [15] introduced an integration architecture enabling service providers to leverage self-sovereign identity solutions effectively. By outlining the technical specifications and integration frameworks, their work facilitates the seamless adoption of decentralized identity technologies across various applications and services.

III. SOFTWARE SPECIFICATIONS

A. Python 3.7.4:

The solid support for sophisticated machine learning libraries required for the creation of sign up wallet is offered by Python 3.7.4. This version optimizes security and speed while guaranteeing compatibility with necessary dependencies. It finds an ideal medium between adding fresh functionality and preserving extensive library support.

B. NumPY:

NumPy is utilized for efficient numerical computations and array operations, aiding in processing user data and interaction logs. Overall, NumPy serves as a foundational tool for numerical tasks within the Sign Up Wallet project, complementing other libraries like TensorFlow and Pandas.

C. Pandas:

Pandas facilitates data preprocessing tasks such as cleaning, normalization, and feature engineering, enhancing the quality of input data for machine

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

learning models. Pandas' powerful data structures and functions streamline data manipulation processes.

D. Wampserver:

WampServer, Configured to host the Flask application locally, providing a development environment for testing and debugging. WampServer's integration with MySQL enables efficient storage and retrieval of user data within the Sign Up Wallet system..

E. Matplotlib:

Employs versatile plotting functions to visualize user interaction data, facilitating insights into user behaviour within the Sign Up Wallet platform. seamlessly with Python scripts to generate dynamic visualizations of real-time registration, verification, and prediction processes within the Sign Up Wallet system.

F. Flask:

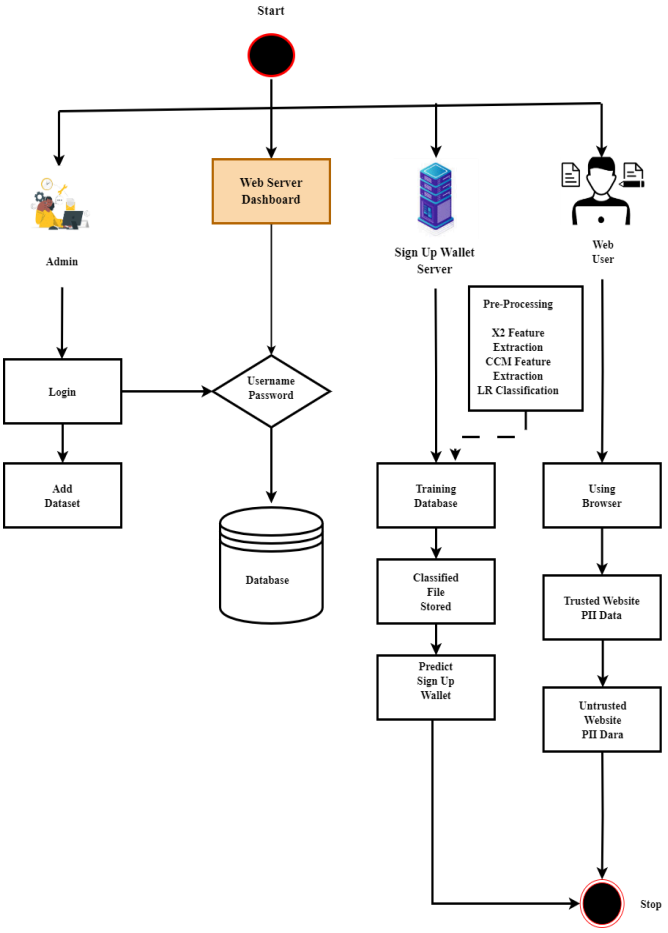
Implements routing, request handling, and business logic for the Sign Up Wallet application, ensuring smooth user interactions and data flow. Flask's lightweight framework allows for easy integration with other Python libraries and tools, facilitating rapid development and deployment.

G. MySQL:

For the Sign up wallet to have a reliable and scalable relational database management system for storing and handling important data, MySQL is required. Its effectiveness in managing big datasets and support for intricate queries guarantees dependable data archiving and retrieval, enabling the program to run smooth.

H. Bootstrap4:

Enhances the frontend user experience with responsive design elements, including navigation menus, forms, and modals. Bootstrap's grid system and CSS components enable rapid prototyping and development of the Sign Up Wallet Web App



IV. Flow Chart

V. PROPOSED WORK

The system flow of the Sign-Up Wallet encapsulates a seamless and secure journey for users as they interact with the platform. Below is a detailed overview of the key steps and interactions within the system:

1. User Registration:

Users initiate the process by registering on the Sign-Up Wallet Web App. During registration, users securely input and store their Personal Identifiable Information (PII) in the Wallet Chain. The Wallet Chain utilizes blockchain technology to ensure the immutability and tamper-resistance of the stored data, while the Logout Module allows users to securely end their sessions. This modular approach ensures a robust, user-centric, and privacy-preserving Sign Up Wallet experience. Credential Verification and Masked Credential Generation Modules ensure secure interactions with service providers, preserving user privacy when needed.

2. Email and Mobile Verification:

The system employs a multi-step verification process to ensure user credibility. Users undergo email verification by clicking on a generated verification link sent to their registered email address. Mobile number verification is conducted through the generation and verification of a

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

One-Time Password (OTP). Wallet Chain generates an E-Mail verification link, which the user receives in their registered E-Mail ID. By clicking on the link, the user confirms the authenticity of their E-Mail ID. An OTP (One-Time Password) is generated and sent to the user's registered Mobile Number. Successful entry of this OTP verifies the legitimacy of the provided Mobile Number.

3. UPI Code Generation:

Upon successful email and mobile verification, the system generates a Unique Personal Identifier (UPI) Code for the user. The UPI Code acts as a unique reference point for the user within the Wallet Chain ecosystem. The Sign-Up Wallet generates a unique URL incorporating the registered website name and the user's UPI Key. This URL serves as a secure and verifiable reference for the registered website. The generated URL is transferred to the Wallet Chain, ensuring the transaction is recorded and verified in the decentralized blockchain environment.

4. Service Provider Interaction:

Users interact with service providers through either the Sign-Up Wallet API, depending on their preference or the platform they are using. Users initiate the prediction process by browsing a website they want to evaluate for trustworthiness. To register the website for prediction, users utilize their Sign-Up Wallet, providing the Unique Personal Identifier (UPI) Key associated with their digital identity.

5. Trusted Website Prediction:

Users initiate trust predictions by browsing a website and registering it for prediction using their Sign-Up Wallet API and UPI Key. The Sign-Up Wallet generates a secure URL incorporating the website name and UPI Key, transferred to the Wallet Chain for verification. The Wallet Chain triggers the trained model to predict the website's trustworthiness, ensuring decentralized and secure predictions.

6. Credential Verification and Submission:

For trusted service providers, the system validates user credentials securely. The process involves UPI Code validation, comprehensive digital identity validation, and granting login access upon successful verification. . The process ensures a secure and privacy-preserving verification for untrusted service providers and provide login credential to access the untrusted service provider

7. Masked Credential Generation and Validation:

Untrusted service providers follow a distinct approach to safeguard user credentials. The system generates a masked credential using a Lookup Substitution Algorithm, ensuring privacy. The masked credential is securely transmitted to untrusted service providers, who validate it without direct access to raw user data. The functionalities encompass the utilization of a secure algorithm, the generation of a masked credential, and the secure transmission of this masked credential to the untrusted service provider. This module facilitates the validation of the masked credential by untrusted service providers without direct access to the user's original credentials. It involves receiving the masked credential, applying the Lookup Substitution Algorithm for decryption or transformation, and validating the decrypted credential without exposing the raw user data

8. Notification Integration:

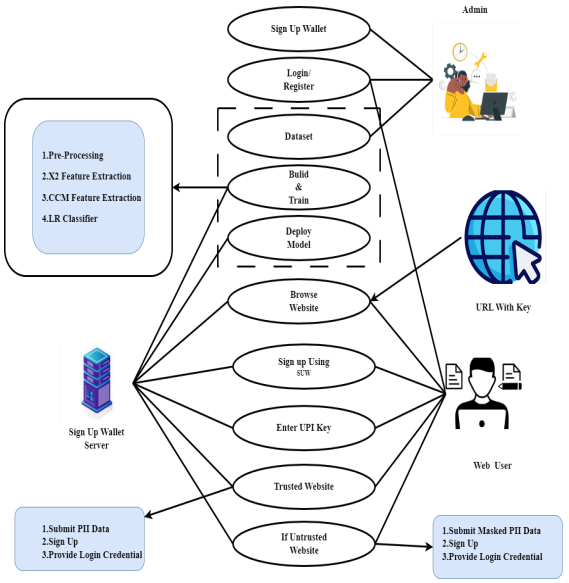
The Notification Module seamlessly integrates with the entire system, providing real-time updates to users on registration, verification, and prediction processes. The Notification Module ensuring timely communication and user engagement. This feature delivers personalized and event-triggered notifications, keeping users informed about activities such as successful verifications and security alerts. Offering multi-channel delivery through in-app messages, emails, and SMS notifications, it caters to user preferences.

9. Traceability Records:

All interactions, whether through the web app or API, are recorded in the immutable and timestamped ledger, ensuring traceability and accountability.

10. User Dashboard Accessibility:

Users, regardless of their registration method, have access to the user-friendly dashboard for oversight and control over their digital identity.



VI. RESULT

The Sign-Up Wallet System is a digital identity management platform designed to provide users with secure and decentralized control over their personal identifiable information (PII). This test report outlines the results of various tests conducted to evaluate the functionality and reliability of the system.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

TC ID	Input	Expected Result	Actual Result	Status
TC001	Valid Admin Credentials	Successful Login	User successfully logged in.	Pass
TC002	Invalid Admin Credentials	Unsuccessful Login with Error Message	Error message displayed: "Invalid credentials."	Pass
TC003	Uploading Dataset for Training	Successful Dataset Upload	Dataset uploaded successfully.	Pass
TC004	Uploading Invalid Dataset Format	Error Message for Invalid Format	Error message displayed: "Invalid file format. Please upload a valid dataset."	Pass
TC005	Admin performs system maintenance tasks.	System maintenance tasks executed without issues.	Admin successfully performs system maintenance.	Pass
TC006	User logs in to the Sign-Up Wallet Web App.	Successful login for the user.	User successfully logs in.	Pass
TC007	User receives login credentials to access the registered website	Successful receipt of login credentials.	User receives login credentials as expected.	Pass

User Empowerment and Control: The project empowers users by providing complete control over their digital identities. This finding indicates a shift towards user-centric digital identity management. Decentralized Blockchain for Data Storage: Utilizing decentralized blockchain technology ensures tamper-resistant data storage, enhancing the security and integrity of user data. Secure and Private Data Handling: The implementation of masked credential generation indicates a focus on secure and private data handling, which is crucial in today's data-sensitive environment. Transparency and Traceability: Blockchain technology ensures transparent and traceable user interactions, enhancing accountability and trust in the system. Machine Learning for Website Trustworthiness: The integration of machine learning to predict website trustworthiness suggests a data-driven approach to enhancing user decision-making and security. Versatile Registration Methods: Accommodating user preferences with versatile registration methods indicates a user-friendly approach to onboarding and identity management. Instant Updates and Oversight: The integrated module providing instant updates and centralized oversight offers users convenient control and visibility into their processes. Reduced Reliance on Centralized Authorities: By reducing reliance on centralized authorities, the project minimizes data vulnerabilities and enhances user autonomy. Trusted Service Providers and Credential Validation: The involvement of trusted service providers in secure credential validation ensures reliability and trustworthiness in the system. Seamless Integration with External Applications: The seamless integration with external applications through the Sign-Up Wallet Registration API enhances interoperability and expands the project's utility. Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

VII. Applications

The project aims to revolutionize the digital landscape by enhancing security, privacy, and user experience through innovative applications. Central to its objectives is the development of a decentralized storage platform leveraging blockchain technology to safeguard user data and ensure secure data handling practices. Additionally, an identity management system will be implemented to streamline registration processes and prioritize user-centric approaches. Utilizing blockchain, the project fosters increased trust and transparency in user interactions, reducing data vulnerabilities through robust security measures and minimizing reliance on centralized authorities. Moreover, machine learning algorithms will empower users with website trustworthiness predictions, enabling informed decision-making for a safer online experience. The project's infrastructure emphasizes interoperability and scalability, facilitating seamless integration with external applications and versatile registration methods to adapt to diverse user needs and accommodate future growth. The project outcomes include enhanced security and privacy for user data through decentralized storage and secure data handling practices.

VIII. Conclusion

The Sign-Up Wallet System represents a significant leap forward in digital identity management, introducing innovative features and technologies to enhance user privacy, security, and control. Through the integration of a secure Wallet Chain, blockchain technology, and machine learning, the system addresses the shortcomings of traditional identity management systems. The Unique Personal Identifier (UPI) Code, generated for each user, serves as a secure reference point within the Wallet Chain ecosystem. Multi-step verification processes, including email and mobile verification, ensure the credibility of user identities. Trusted service providers can efficiently verify user credentials using the UPI Code, streamlining the registration process. For untrusted service providers, the system employs a privacy-preserving approach by generating masked credentials using a Lookup Substitution Algorithm. This protects user data while allowing secure verification by untrusted entities. The future enhancements for the Sign-Up Wallet System are strategically geared towards enhancing security, expanding utility, and offering users greater control over their digital identities. These include the integration of advanced biometric authentication methods for heightened security, an expanded range of use cases beyond website trust prediction, and user-controlled data sharing capabilities. Additionally, the development of a dedicated mobile wallet application aims to provide users

with seamless and secure management of their digital identities on- the-go.

IX. 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.

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. A. 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.