IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204323 |

Sign Up Wallet a Block Chain based Personally Identifiable Information (PII) Masking using Lookup Substitution

K.Suvalakshmi, D.Sabithra, K.Sindhubairavi , S.Sarmathi, Ms.S.Sharmila,

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, TamilNadu, India

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, TamilNadu, India

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, TamilNadu, India

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, TamilNadu, India

Assistant Professor, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, TamilNadu,India

ABSTRACT: Digital identity is a user's online identification, similar to a physical identification card such as a passport or driver's license. A digital identity contains characteristics or attributes of the user. As we access apps and websites, organizations are dominantly using centralized and federated identity management systems (e.g. signing in with a Google or Facebook account) by default. The centralized system puts data at risk of large scale hacks and breaches while the federated model enables companies to track user data without their knowledge. Existing identity management systems either use a centralized authentication server or rely on identity providers to authenticate users for gaining access to various services. These systems have failed to safeguard user data privacy and do not encourage the portability of identity data. A trustworthy and reliable system is needed so that individuals can interact and network digitally and securely. These problems are motivated the development of the Sign Up Wallet a blockchain and machine learning based Self-Sovereign Identity model to manage digital identities. The emerging blockchain technology enables self-sovereign identity management, a decentralized identity management model that eliminates identity providers as a trusted third party and machine learning is used to find the trusted service provider. In this proposed system users store their digital identity in a Sign Up Wallet with cryptographic keys. When registering with a trusted service provider, a Unique Personal Identifier (UPI) Code is submitted for direct credential verification. Logistic Regression is used for predicting whether a website is trusted or not. If the service provider is untrusted, a masked credential isgenerated using a Lookup Substitution Algorithm, preserving privacy during verification.

I. INTRODUCTION

Sign up is a phrase referring to the creation of an online account using an e-mail address or a username and password. The online account is usually for a website or web-based service. Once someone has signed up for a service, they can access their accountby logging in. A signup form is a web page, popup, or modal where users enter the information required to access that website's services. The information collected is determined by the nature of the website and the services it offers. Most signup forms requirea name, email address, username, and password.
It is also an important part of customer acquisition and retention strategy. It is a useful tool that can be used across several marketing channels, including social media platforms as well as blogs and websites.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204323 |

II. LITERATURE SURVEY

1: A Self-Sovereign Identity Based on Zero-Knowledge Proof and BlockchainAuthor: Mohameden Dieye, Pierre Valiorgue Year:2023

Objective: Self-Sovereign Identities (SSI) using two Zero-Knowledge Proof (ZKP) protocols based onthe discrete logarithm difficulty..

Merits:

- Self-Sovereign Identity solution with Zero-Knowledge Proof based on blockchaintechnologies
- **Demerits:**
- Provided information does not explicitly mention any demerits or limitations of theproposed solution

2:Comparative Analysis of Decentralized Identity ApproachesAuthor:Morteza Alizadeh, Karl Andersson, Olov Schelén Year:2022

Objective: Focus is on providing user with control over their information and biometrics in adecentralized manner

Merits:

- Decentralized identification, emphasizing user control over information and biometric.
- **Demerits:**
- Specific algorithms or details of the machine learning model (BioIPFS) are notthoroughly explained in the provided text.

3. 3:Blockchain Data Privacy Protection and Sharing Scheme Based onZero-Knowledge Proof
Author: Tao Feng, PuYang, Chunyan LiuYear:2022
Objective:
Blockchain privacy protection scheme based on zero-knowledge proof to securely

Merits:
Achieves privacy protection through a zero-knowledge proof-based scheme..

Demerits:
Potential limitations may arise based on the specific implementation.

III. EXISTING SYSTEM

Traditional Registration Process
The traditional registration process for digital identities typically involves a centralized approach where users submit their personal information to a service provider. This information may include details such as name, email address, and password.During registration, users are required to create credentials, usually in the form of a username and password, which they use for subsequent logins. While this method is widespread, it has inherent security and privacy concerns .The centralized storage of user data makes it a target for large-scale hacks and data breaches, putting users at risk of identity theft and other malicious activities

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204323 |

Decentralized or distributed Public Key Infrastructure (dPKI)
Thus approach is to managing digital identities and public keys in a manner that distributes trust and authority across a network rather than relying on a central authority. Traditional PKI relies on a central Certificate Authority (CA) to issue and manage digital certificates, which can introduce vulnerabilities and single points of failure.

E-Wallet
The E-wallet architecture serves as a foundational framework tailored for the financial sector, specifically catering to banks and financial institutions. Built upon the robust Distributed Ledger Technology (DLT), this architecture introduces a decentralized approach to managing digital assets and financial transactions. At its core, the E-wallet architecture employs a distributed ledger, ensuring that transaction records are securely maintained across a network of nodes. This decentralized nature adds an extra layer of security, making the system resistant to tampering and unauthorized alterations.

Elliptic Curve Digital Signature Algorithm
The Elliptic Curve Digital Signature Algorithm (ECDSA) is a prominent asymmetric cryptographic algorithm designed for digital signatures, offering a high level of security with relatively shorter key lengths compared to alternative algorithms. Its security foundation is rooted in the mathematical properties of elliptic curves over finite fields. The algorithm involves the use of a private key known only to the entity generating the signature and a corresponding public key, which is openly shared and used for signature verification

RSA
The service provider stores this data in a centralized authentication server, which becomes the authoritative source for verifying user identities. During registration, users are required to create credentials, usually in the form of a username and password, which they use for subsequent logins.

IV. PROPOSED SYSTEM

Self-Sovereign Identity Management:
Sign Up Wallet introduces a paradigm shift by enabling users to store their digital identity ina self-sovereign manner. This means users have complete ownership and control over their identity without relying on intermediaries.

Blockchain Technology
The core of the system lies in blockchain technology, ensuring a decentralized and tamper- resistant ledger for storing digital identities. The blockchain provides transparency, immutability, and traceability, mitigating the risks associated with centralized datarepositories.

Machine Learning for Trusted Website Prediction
The integration of machine learning, specifically Logistic Regression, empowers users to predict the trustworthiness of websites. This predictive capability adds an extra layer of security, allowing users to make informed decisions about the reliability of online platforms.

Flexible Registration
The system accommodates various user preferences by offering flexible registration methods. Users can choose to register through the intuitive Sign Up Wallet Web App or seamlessly integrate with external applications using the Sign Up Wallet Registration API.

Secure Credential Verification
Trusted service providers employ a robust verification process, ensuring the security of user credentials. This involves validating the Unique Personal Identifier (UPI) Code and scrutinizing different facets of the user's digital identity stored in the WalletChain.

Privacy-Preserving Credential Handling
For interactions with untrusted service providers, the system employs advanced privacymeasures. A masked credential, generated through a Lookup Substitution Algorithm, shields user data during verification, prioritizing privacy without compromising security.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204323 |

Notification Module Integration

Real-time communication is facilitated through the seamless integration of the Notification Module. Users receive instant updates on their registration, verification, and prediction processes, enhancing overall user experience and transparency.

Traceability and Accountability

The decentralized blockchain ledger ensures every user interaction is recorded with precision. This not only enhances traceability but also establishes a robust system of accountability for all transactions within the network.

User-Friendly Dashboard

Users are provided with a user-friendly dashboard, irrespective of their chosen registration method. This dashboard serves as a centralized hub, offering users oversight and control over their digital identities.

Advantages

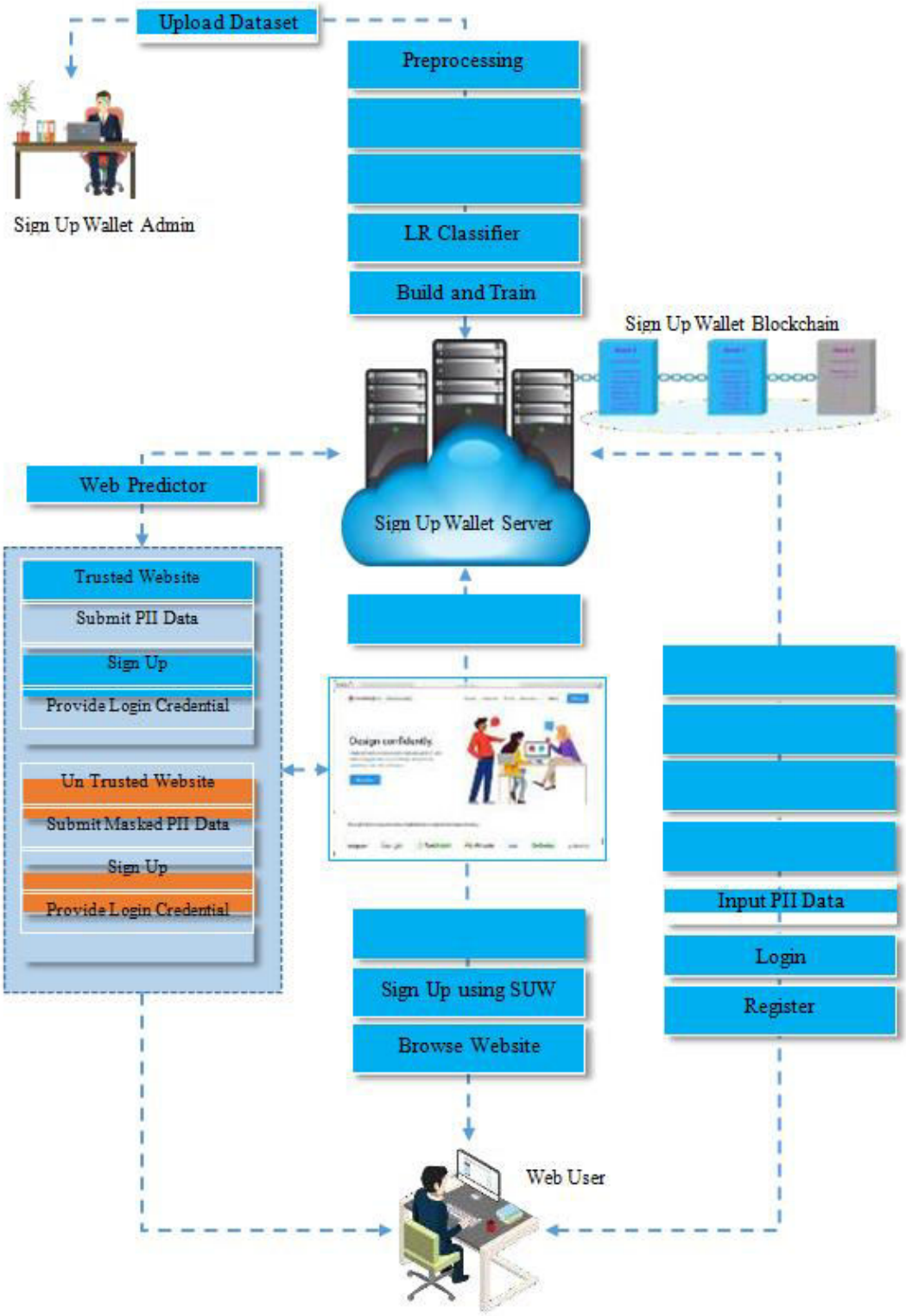
- Empowers users with complete control over their digital identities.
- Utilizes decentralized blockchain for tamper-resistant data storage.
- Implements masked credential generation for secure and private data handling.
- Blockchain ensures transparent and traceable user interactions.
- Machine learning predicts website trustworthiness for informed decisions.
- Accommodates user preferences with versatile registration methods.
- Integrated module provides instant updates on user processes.
- Centralized hub offers convenient oversight and control for users.
- Reduces reliance on centralized authorities, minimizing data vulnerabilities.
- Trusted service providers conduct secure credential validation.
- Blockchain ledger ensures data integrity and prevents unauthorized changes.
- Seamlessly integrates with external applications through Sign Up Wallet RegistrationAPI.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204323 |



V. 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. The Unique Personal Identifier

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204323 |

(UPI) Code, generated for each user, serves as a secure reference point within the WalletChain ecosystem.. 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 use of machine learning, particularly Logistic Regression, for Trusted Website Prediction adds an additional layer of security by distinguishing trusted websites from potentially untrustworthy ones.

VI. FUTURE WORK

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. These enhancements collectively reinforce the system's versatility, security, and user-centric design, aligning it with evolving technological trends and user expectations in the realm of digital identity management.

REFERENCES

1. EIP-712: Ethereum Typed Structured Data Hashing and Signing. Accessed: Mar. 3, 2023. [Online]. Available:
2. https://eips.ethereum.org/ EIPS/eip-712
3. B. Podgorelec, L. Alber, and T. Zefferer, ‘‘What is a (Digital) identity wallet?Asystematicliterature review,’’ in Proc. IEEE 46th
4. Annu. Comput., Softw., Appl. Conf. (COMPSAC), Jun. 2022, pp. 809–818.
5. Š. Cucko and M. Turkanovic, ‘‘Decentralized and self-sovereign identity: Systematicmapping study,’’ IEEE Access, vol. 9, pp.
6. 139009–139027, 2021.
7. A. M. Antonopoulos and G. Wood, Mastering Ethereum: Building Smart Contracts andDapps. Newton, MA, USA: O’reilly Media, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details