Vol-08 Issue 08, August -2024

ISSN: 2456-9348
Impact Factor: 7.936

International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

SIGN UP WALLET A BLOCK CHAIN BASED PERSONALLY IDENTIFIABLE INFORMATION (PII) MASKING USING LOOKUP SUBSTITUTION

Miss. Shalini.S,
II MCA, Sri Muthukumaran Institution Of Technology, Mangadu, Chennai
DR. Pandian.E
Assistant Professor, Sri Muthukumaran Institution Of Technology, Mangadu, Chennai

ABSTRACT

Digital identity is akin to a digital version of a physical ID, such as a passport or driver's license, containing various attributes that represent a user online. Currently, centralized and federated identity management systems, such as those enabling logins via Google or Facebook, dominate the digital landscape. While these systems simplify access, they pose significant risks. Centralized systems are vulnerable to large-scale data breaches, and federated models often allow companies to track user data without consent. Existing identity management approaches either rely on centralized servers or entrust identity providers with user authentication, often compromising data privacy and hindering the portability of identity information. To address these challenges, a more secure and reliable system is necessary—one that empowers users to manage their digital identities independently and securely. This need has driven the development of the Sign Up Wallet, a Self-Sovereign Identity (SSI) model utilizing blockchain and machine learning to safeguard digital identities. Blockchain technology supports decentralized identity management, removing the need for third-party identity providers, while machine learning identifies trusted service providers. Users store their digital identity within the Sign Up Wallet using cryptographic keys. When interacting with a service provider, they submit a Unique Personal Identifier (UPI) for direct credential verification. To assess the trustworthiness of websites, Logistic Regression is employed. If a service provider is deemed untrustworthy, a masked credential is generated using a Lookup Substitution Algorithm, ensuring privacy during the verification process. This approach allows for secure verification without exposing sensitive data, granting individuals greater control over their digital identities and reducing reliance on centralized authorities, thus minimizing the risks of data breaches and privacy infringements.

Keywords:
Digital identity, Centralized identity management, Federated identity management, Data privacy, Block chain, Machine learning, Sign Up Wallet.

(1) INTRODUCTION

"Sign up" refers to the process of creating an online account by providing an email address, username, and password, typically to access a website or web-based service. After signing up, users can log in to access their account. A signup form is the interface where users enter the necessary information to gain access to a website's services. The specific details requested in a signup form vary depending on the nature of the website and its offerings, but most commonly include a name, email address, username, and password.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

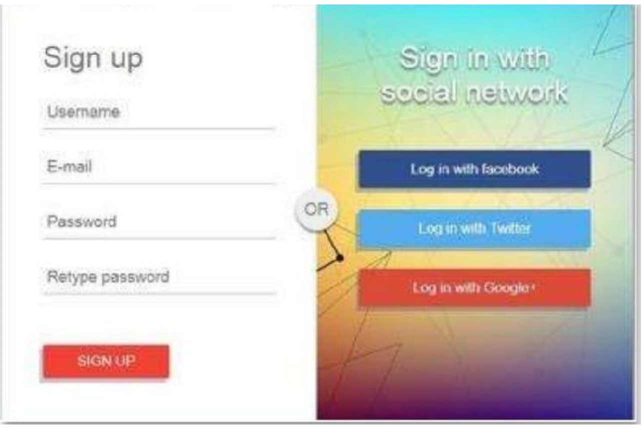


Figure1.1. Sign in with Social Network

Signup forms are crucial components of any website, serving multiple purposes based on the business's goals. They can be used to generate leads, collect emails for newsletters, and attract new customers. However, many businesses overlook the importance of optimizing their signup forms for conversion, which can limit their effectiveness. Despite this, signup forms remain a valuable tool for generating leads, especially in 2020. They are vital for building a list of engaged, permission-based subscribers and play a key role in customer acquisition and retention strategies. Additionally, signup forms can be leveraged across various marketing channels, including social media platforms, blogs, and websites, making them a versatile asset for any business.

(2) TYPES OF EMAIL SIGN-UP FORM

1. *Email Sign-Up Forms*: Collect email addresses to grow your email list and generate leads.
2. *Product Sign-Up Forms*: Essential for e-commerce, these forms are used before a purchase, focusing on clarity, product display, and security.
3. *Subscription Sign-Up Forms*: Key for subscription-based businesses; these forms aim to convert users by offering demos or free trials.
4. *Service Sign-Up Forms*: Designed to convert visitors into users, often using social media sign-up options.

(3) SYSTEM SPECIFICATION

3.1. HARDWARE REQUIREMENTS

Server/Computing Power: Multi-core processors: Intel Xeon, AMD Ryzen.
RAM: 16GB or higher for concurrent transactions and machine learning.
Storage: 256 Solid State Drives (SSD) for swift data access.

3.2. SOFTWARE REQUIREMENTS

□

Web Development
– Web server software: Apache, Nginx.
– Front-end Client: HTML, CSS, JavaScript.
– Front-end Server: Python
– Web Framework: Flask

Database Management System
– MySQL

□ **Blockchain Platform:**
– JSON

□ **Machine Learning Framework:**
– TensorFlow, PyTorch, or scikit-learn.

□ **Programming Languages:**
– Python for machine learning and backend.
– Solidity for smart contract development.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

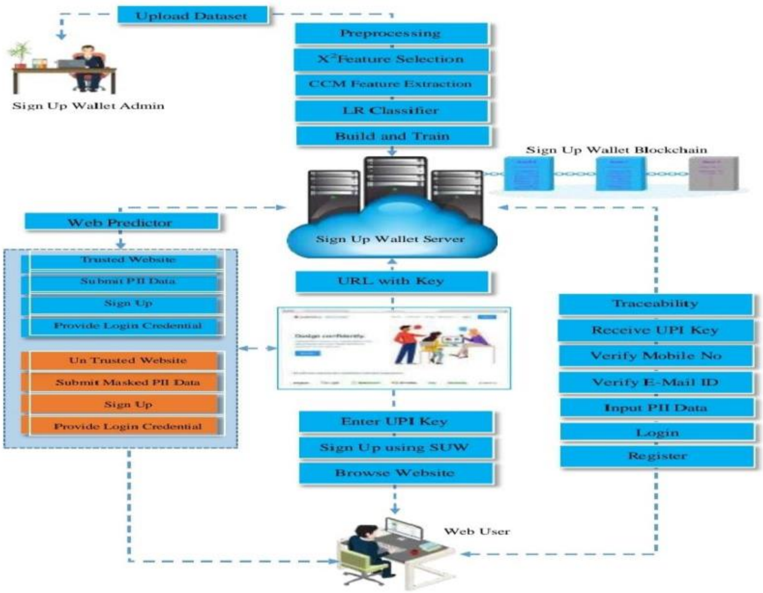
(4) EXISTING SYSTEMS

1. *Traditional Registration Process*: Centralized method where users provide personal info (e.g., name, email, password) to a service provider, stored in a central server. Vulnerable to security breaches and identity theft.
2. *Decentralized Public Key Infrastructure (dPKI)*: Distributes trust and authority across a network instead of relying on a central authority, reducing vulnerabilities.
3. *E-Wallet*: A decentralized financial architecture using Distributed Ledger Technology (DLT) for secure, tamper-resistant transaction records across multiple nodes.
4. *Elliptic Curve Digital Signature Algorithm (ECDSA)*: A cryptographic algorithm for digital signatures that uses elliptic curves, offering strong security with shorter key lengths.
5. *RSA (Rivest–Shamir–Adleman)*: A foundational asymmetric cryptography algorithm for secure data transmission and digital signatures, based on the difficulty of factoring large numbers.

(5) PROPOSED SYSTEM

1. *Self-Sovereign Identity Management*: Users have full control and ownership of their digital identities without intermediaries.
2. *Blockchain Technology*: Utilizes a decentralized, tamper-resistant blockchain ledger for secure and transparent digital identity storage.
3. *Machine Learning for Trusted Website Prediction*: Integrates Logistic Regression to predict website trustworthiness, enhancing user security.
4. *Flexible Registration*: Offers registration via the Sign Up Wallet Web App or through external applications using an API.
5. *Secure Credential Verification*: Trusted service providers verify user credentials, including a Unique Personal Identifier (UPI) Code, ensuring security.
6. *Privacy-Preserving Credential Handling*: Uses a Lookup Substitution Algorithm to mask user data during verification with untrusted providers, prioritizing privacy.
7. *Notification Module Integration*: Provides real-time updates on registration, verification, and prediction processes for enhanced user experience.
8. *Traceability and Accountability*: The blockchain ledger records every interaction, ensuring traceability and accountability.
9. *User-Friendly Dashboard*: Offers a centralized hub for users to manage and control their digital identities easily.

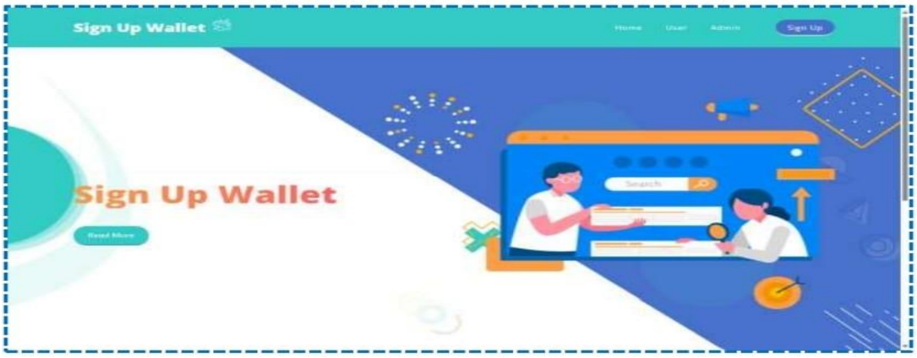
(6) SYSTEM ARCHITECTURE



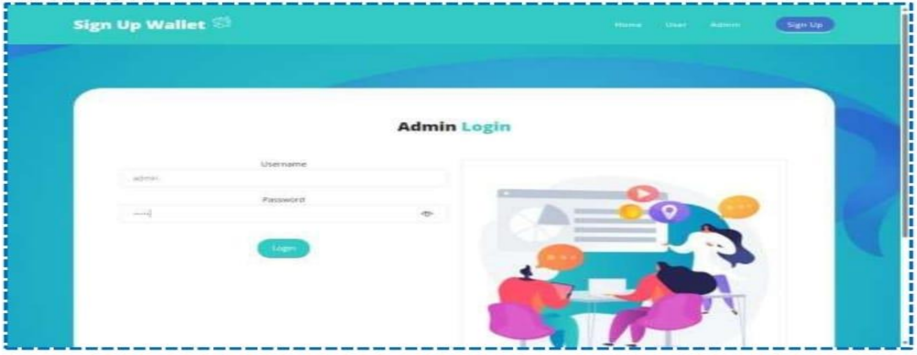
IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

(7) SCREEN SHOT

HOME PAGE



ADMIN LOGIN

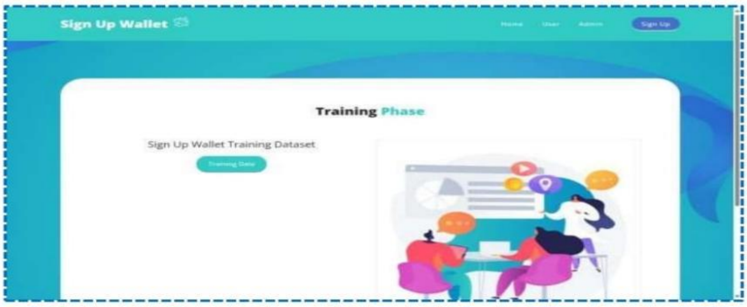


Admin Login

Username: admin

Password: ••••|

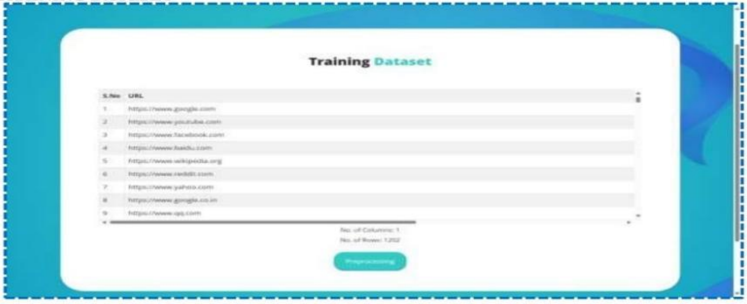
TRAIN PHASE



Training Phase

Sign Up Wallet Training Dataset

TRAINING DATESET



Training Dataset

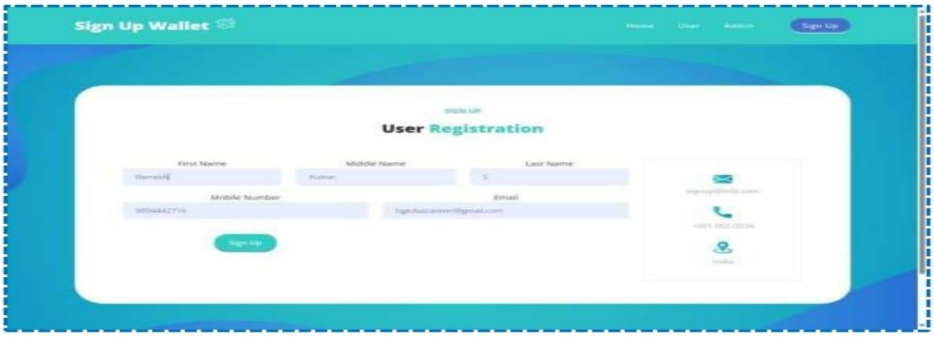
S.No	URL
1	https://www.google.com
2	https://www.youtube.com
3	https://www.facebook.com
4	https://www.baidu.com
5	https://www.wikipedia.org
6	https://www.reddit.com
7	https://www.yahoo.com
8	https://www.google.co.in
9	https://www.qq.com

No. of Columns: 1

No. of Rows: 1202

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

USER REGISTRATION

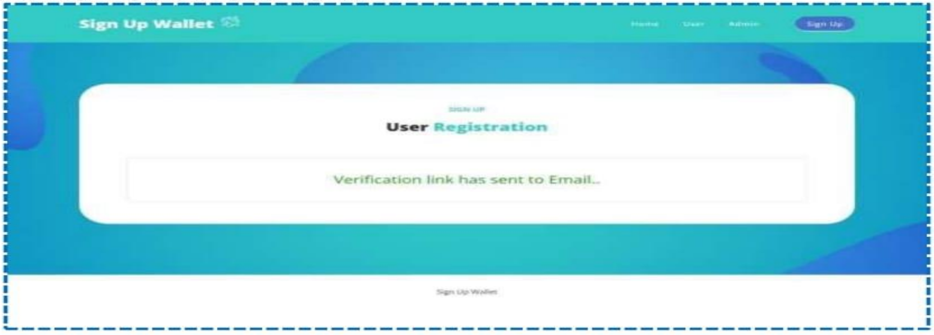


SIGN UP

User Registration

First Name: Ramesh
Middle Name: Kumar
Last Name: S
Mobile Number: [illegible]
Email: [illegible]

VERIFICATION LINK SENT TO EMAIL



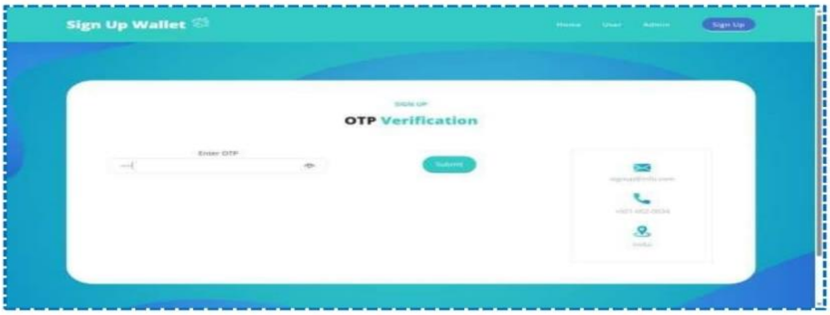
SIGN UP

User Registration

Verification link has sent to Email..

Sign Up Wallet

OTP VERIFICATION

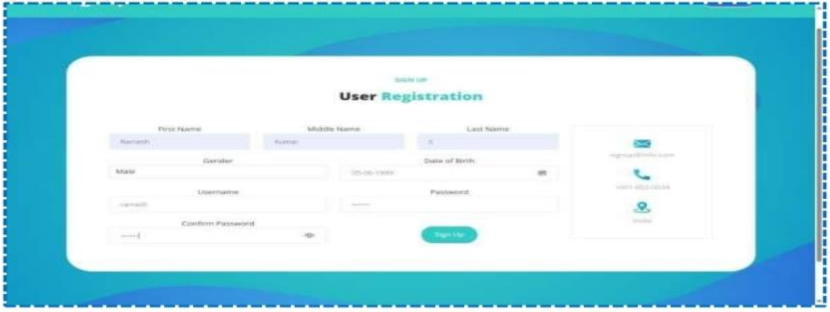


SIGN UP

OTP Verification

Enter OTP

USER REGISTRATION AND INFORMATION



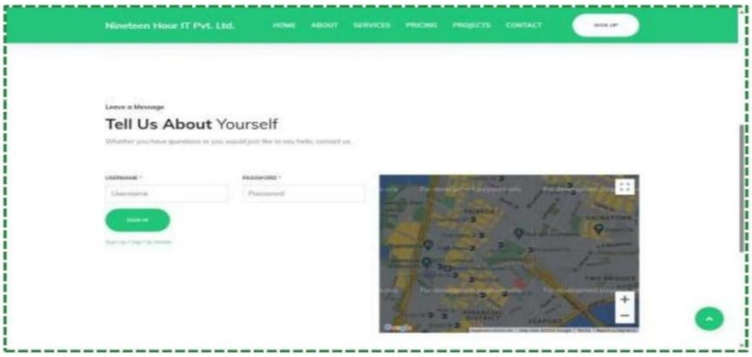
SIGN UP

User Registration

First Name: Ramesh
Middle Name: Kumar
Last Name: S
Gender: Male
Date of Birth: [illegible]
Username: ramesh
Password
Confirm Password

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

TELL US ABOUT YOURSLEF



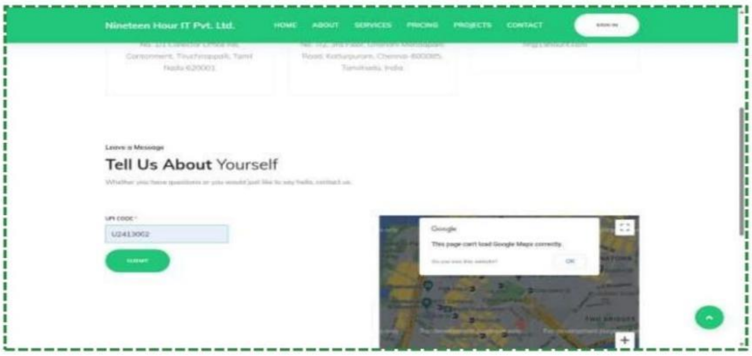
Leave a Message

Tell Us About Yourself

Whether you have questions or you would just like to say hello, contact us.

USERNAME * Username

PASSWORD * Password



Cantonment, Tiruchirappalli, Tamil Nadu 620001

Road, Kotturpuram, Chennai-600085, Tamilnadu, India

Leave a Message

Tell Us About Yourself

Whether you have questions or you would just like to say hello, contact us.

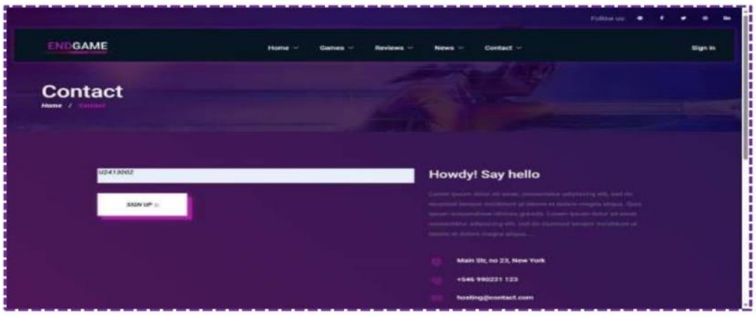
UPI CODE * U2413002

Google

This page can't load Google Maps correctly.

Do you own this website?

CONTACT PAGE



Contact

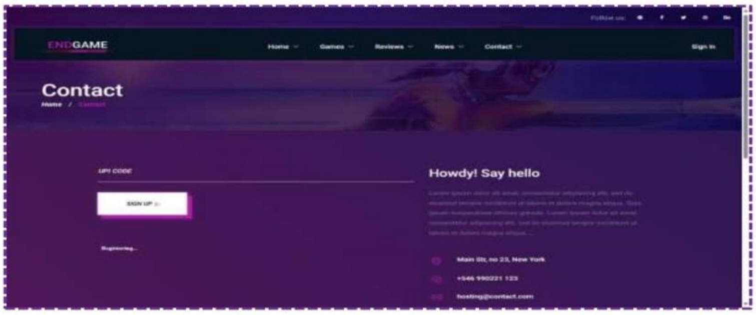
U2413002

Howdy! Say hello

Main Str, no 23, New York

+546 990221 123

hosting@contact.com



Contact

UPI CODE

Registering...

Howdy! Say hello

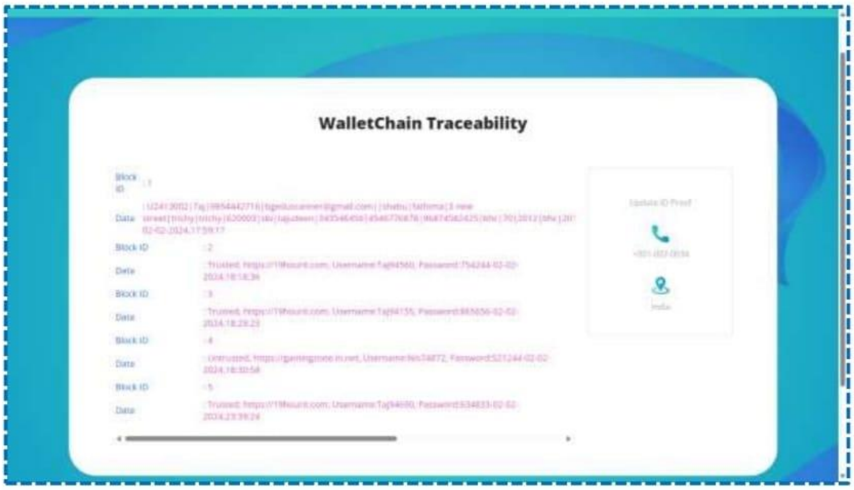
Main Str, no 23, New York

+546 990221 123

hosting@contact.com

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

WALLET CHAIN TRACEABILITY



WalletChain Traceability

Block ID : 1
Data : U2413002 | Taj | 9854442718 | [illegible]@gmail.com | | shabu | fathima | 3 new street | trichy | trichy | 620003 | [illegible] 02-02-2024,17:59:17
Block ID : 2
Data : Trusted, https://19hoursi.com, Username:Taj94560, Password:754244-02-02-2024,18:18:36
Block ID : 3
Data : Trusted, https://19hoursi.com, Username:Taj94155, Password:865656-02-02-2024,18:29:23
Block ID : 4
Data : Untrusted, https://gamingzone.in.net, Username:[illegible], Password:521244-02-02-2024,18:30:58
Block ID : 5
Data : Trusted, https://19hoursi.com, Username:Taj94690, Password:534833-02-02-2024,23:39:24

(8) CONCLUSION

The Sign Up Wallet System marks a substantial advancement in digital identity management by introducing cutting-edge features and technologies designed to bolster user privacy, security, and autonomy. By leveraging the secure Wallet Chain, blockchain technology, and machine learning, the system overcomes the limitations of traditional identity management models. Each user is assigned a Unique Personal Identifier (UPI) Code, which serves as a secure anchor within the Wallet Chain network. Multi-step verification methods, including email and mobile confirmation, ensure the authenticity of user identities. Trusted service providers can easily verify user credentials using the UPI Code, simplifying the registration process. For interactions with untrusted service providers, the system employs a privacy-preserving mechanism that generates masked credentials through a Lookup Substitution Algorithm, safeguarding user data while still allowing secure verification. Machine learning, specifically Logistic Regression, is utilized to predict the trustworthiness of websites, adding another layer of security by identifying reliable sites. Ultimately, the Sign Up Wallet System gives users enhanced control over their digital identities, offering a secure, decentralized, and user-focused solution that addresses existing challenges and sets a new benchmark for the future of digital identity management.

(9) FUTURE ENHANCEMENT

Future enhancements for the Sign Up Wallet System are strategically focused on strengthening security, broadening its applications, and providing users with even greater control over their digital identities. Planned upgrades include the integration of advanced biometric authentication to further enhance security, an expanded array of use cases beyond website trust prediction, and user-directed data sharing features. Additionally, the introduction of a dedicated mobile wallet app is set to offer users seamless and secure management of their digital identities while on the move. These enhancements will collectively enhance the system's versatility, security, and user-centric design, ensuring it remains in step with evolving technological advancements and user expectations in the digital identity management space.

(11)REFERENCE

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 forself-sovereign identity", Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA),pp. 1-5, Sep. 2019.
16.M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O‘Donnell and D. Reed, "The trust over IP stack", IEEE Commun. Standards Mag., vol. 3, no. 4, pp. 46-51, Dec. 2019.
17.R. Soltani, U. T. Nguyen and A. An, "A new approach to client onboarding using selfsovereign identity and distributed ledger", Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData), pp. 1129-1136, Jul. 2018.
18.W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou and H. Jin, "SBLWT: A secure blockchain lightweight wallet based on trustzone", IEEE Access, vol. 6, pp. 40638-40648, 2018.
19.J. Su, A. Shukla, S. Goel and A. Narayanan, "De-anonymizing web browsing data with social networks", Proc. 26th Int. Conf. World Wide Web, pp. 1261-1269, 2017.
20.X. Zhu, Y. Badr, J. Pacheco and S. Hariri, "Autonomic identity framework for the Internet of Things", Proc. Int. Conf. Cloud Autonomic Comput., pp. 69-79, 2017.