



e-ISSN:2582-7219



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521



6381 907 438



6381 907 438



ijmrset@gmail.com



www.ijmrset.com



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

Ms. G. Sivagami, AP/MCA, Dr. T. Geetha MCA., M.Phil., Ph.D., Mr. S. S. Nishanthan MCA

Assistant Professor, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

HOD, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

PG Student, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

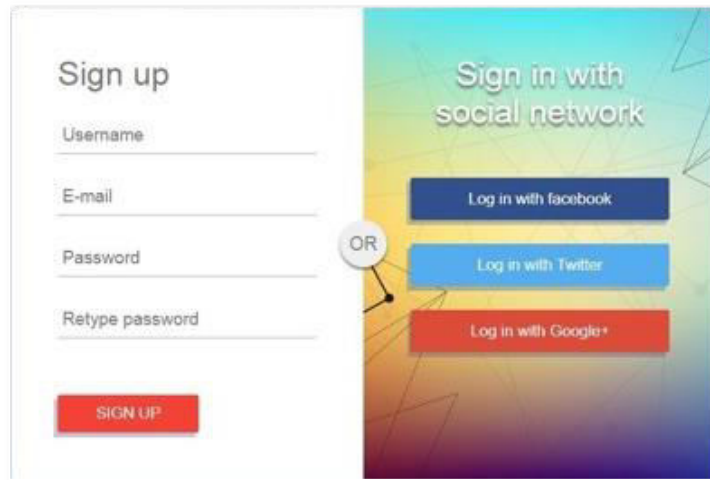
ABSTRACT: Digital identity is a user's online identification, similar to a physical identification card such as a passport or driver's license. A digital identity contains characteristics or attributes of the user. As we access apps and websites, organizations are dominantly using centralized and federated 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 is generated using a Lookup Substitution Algorithm, preserving privacy during verification. This masked credential is then provided to the service provider, allowing verification without exposing the raw data and maintaining user security. The primary goal of this project is to give individuals greater control over their own digital identities, reducing the reliance on centralized authorities and minimizing the risks associated with data breaches and privacy violations.

KEYWORDS: Block chain, Machine Learning, APIs

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 account by 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 require a name, email address, username, and password.

Sign-up Forms are an integral part of any website. Depending on the nature of business, forms can be used for generating leads, collecting emails for newsletter, and acquiring new customers. The problem is that a lot of businesses do not bother to optimize their forms for conversion. forms are still very valuable in generating leads for business in 2020. A form is essential in growing a list of permission-based, engaged subscribers. 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.



The image shows a user interface for a sign-up and login process. On the left, there is a 'Sign up' form with four input fields: 'Username', 'E-mail', 'Password', and 'Retype password'. Below these fields is a red 'SIGN UP' button. On the right, there is a 'Sign in with social network' section with three buttons: 'Log in with facebook' (dark blue), 'Log in with Twitter' (light blue), and 'Log in with Google+' (red). A white circle with the text 'OR' is positioned between the sign-up form and the social login buttons, indicating an alternative login method.

Fig 1: Sign-Up Form

II. 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. 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. While this method is widespread, it has inherent security and privacy concerns.

III. LITERATURE SURVEY

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a ‘digital ledger.’ Blockchain is a method of recording information that makes it impossible or difficult for the system to be changed, hacked, or manipulated. A blockchain is a distributed ledger that duplicates and distributes transactions across the network of computers participating in the blockchain.

Blockchain is a type of DLT. Each transaction stored in the blockchain is called a block. Each block is chained to the previous block using a cryptographic hash. So, if someone wants to tamper with a certain block, they have to tamper with all the previous blocks in the chain, which is impossible/ extremely difficult since all peers have the same ledger, and any change is noticeable. This creates an immutable record of blocks, that does not require an external authority. Hence, in the simplest terms, a blockchain is a chain of blocks. It is a process or technology of recording information as blocks that makes it impossible to change, hack, or cheat.

Blockchain Structure

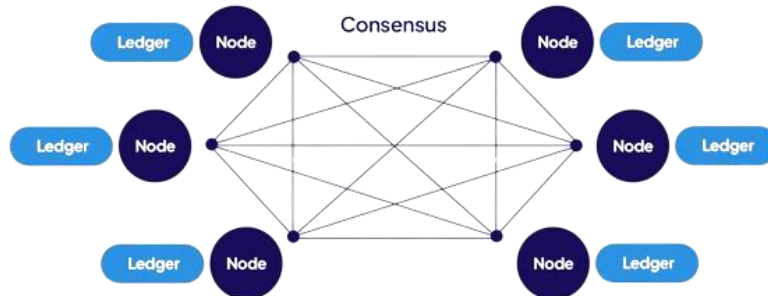


FIG 2: BLOCKCHAIN STRUCTURE

MACHINE LEARNING: Machine learning (ML) is a discipline of artificial intelligence (AI) that provides machines with the ability to automatically learn from data and past experiences while identifying patterns to make predictions with minimal human intervention. Machine learning algorithms are molded on a training dataset to create a model. As new input data is introduced to the trained ML algorithm, it uses the developed model to make a prediction.

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.

IV. PROPOSED SYSTEM

The Sign-Up Wallet is an innovative Self-Sovereign Identity (SSI) model designed to address the limitations of current centralized and federated identity management systems.

Sign Up Wallet: Users store their digital identity in a Sign-Up Wallet, leveraging cryptographic keys for secure storage. This wallet acts as a decentralized repository, enhancing data privacy and control.

Unique Personal Identifier (UPI) Code: During registration with a trusted service provider, users submit a UPI Code for direct credential verification. This streamlines the authentication process and ensures a secure connection between the user and the trusted service.

Logistic Regression for Trusted Website Prediction: Logistic Regression is employed to predict the trustworthiness of service providers. This algorithm, trained on relevant features, helps determine whether a website is trusted or not, providing an additional layer of security.

Lookup Substitution Algorithm for Untrusted Service Providers: In instances where the service provider is untrusted, a Lookup Substitution Algorithm generates a masked credential. This preserves user privacy during verification, as the actual credentials remain secure.

BLOCK CHAIN BASED FOR SIGN-UP WALLET

The Integration with Blockchain Module ensures decentralized and tamper-resistant data storage, 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.



Wallet Chain Integration: In this module the integration of the Wallet Chain as a blockchain with the Sign-Up Wallet Web App, various modules collaborate to form a secure and decentralized ecosystem, enhancing Digital identity management.

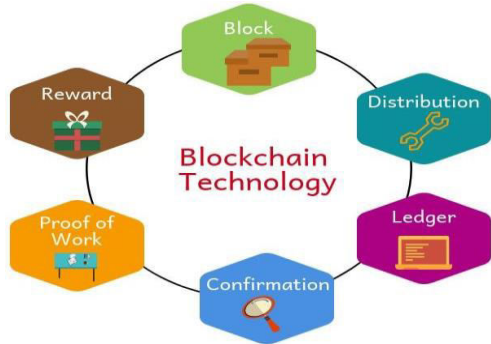


Fig 3: Blockchain Technology

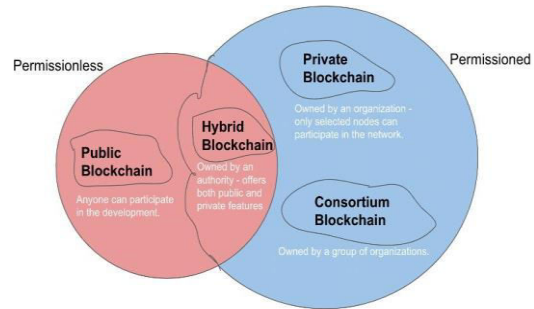


Fig 4: Blockchain Networks

Trusted Website Classification: Building and training a Trusted Website Classification system using Logistic Regression involves several key modules to ensure accuracy, efficiency, and reliability in predicting the trustworthiness of websites.

Sign Up Wallet Registration API: The Sign-Up Wallet Registration API process is designed to provide a secure and versatile mechanism for users to manage their digital identity. The modules ensure that user credentials are handled with utmost privacy and that access to trusted and untrusted service providers is managed effectively.

Wallet Chain Traceability: Wallet Chain Traceability is a foundational feature within the Sign-Up Wallet system, ensuring transparency and accountability in digital identity management. Every transaction, from data updates to UPI Code generation, is securely recorded in an immutable ledger with precise timestamps. This user-centric approach allows individuals to self-verify their transaction history, promoting transparency and trust.

Notification: 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.

SYSTEM ARCHITECTURE:

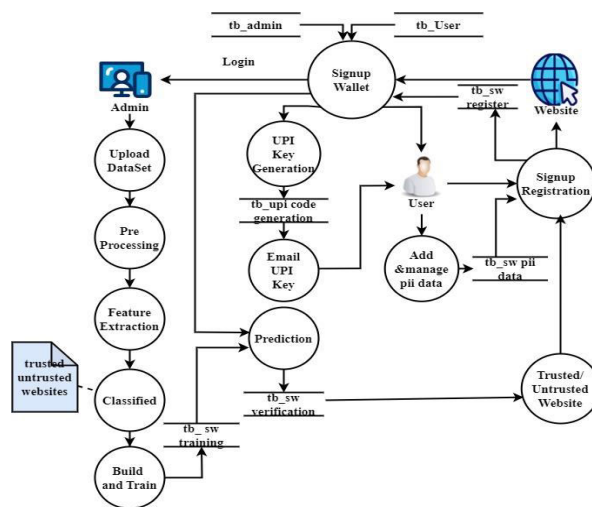


FIG 5: SYSTEM ARCHITECTURE



The Sign-Up Wallet system represents an advancement in the digital identity management, providing users with a secure and user-centric platform. At its core, the system introduces the concept of a Wallet Chain, a digital wallet fortified by blockchain technology. This Wallet Chain serves as a highly secure repository for users to store their Personal Identifiable Information (PII), personal attributes, and other relevant data. Users initiate their interaction with the system through the Sign-Up Wallet Web App, where they securely store their digital identity within the Wallet Chain. Blockchain technology ensures the immutability and tamper-resistant nature of the stored data, offering a robust solution for safeguarding sensitive information. The system introduces the innovative concept of a Unique Personal Identifier (UPI) Code. This code acts as a unique reference point for each user within the Wallet Chain ecosystem. The registration process incorporates multi-step verification, ensuring the credibility of users. Email verification links and One-Time Passwords (OTPs) for mobile numbers add layers of security, providing a thorough authentication process. Trusted service providers can directly verify user credentials by utilizing the UPI Code, streamlining the registration process and ensuring a seamless user experience. On the other hand, for untrusted service providers, the system employs a privacy-preserving approach. Instead of exposing actual credentials, a masked credential is generated using a Lookup Substitution Algorithm. This algorithm transforms or encrypts user credentials, allowing verification without exposing raw data. The system harnesses the power of machine learning, specifically Logistic Regression, to predict the trustworthiness of websites.

This predictive model aids in distinguishing trusted websites from potentially untrustworthy ones, contributing to enhanced security during user interactions. The overarching goal of the Sign-Up Wallet system is to empower individuals with greater control over their digital identities. This innovative approach addresses the inherent vulnerabilities of centralized and federated identity management systems. By prioritizing user privacy, security, and seamless interaction with online services, the Sign-Up Wallet system emerges as a transformative force in the landscape of digital identity management. Through the fusion of blockchain, machine learning, and user-centric design principles, it not only mitigates existing challenges but also sets a new standard for the future of digital identity ecosystems.

V. RESULT

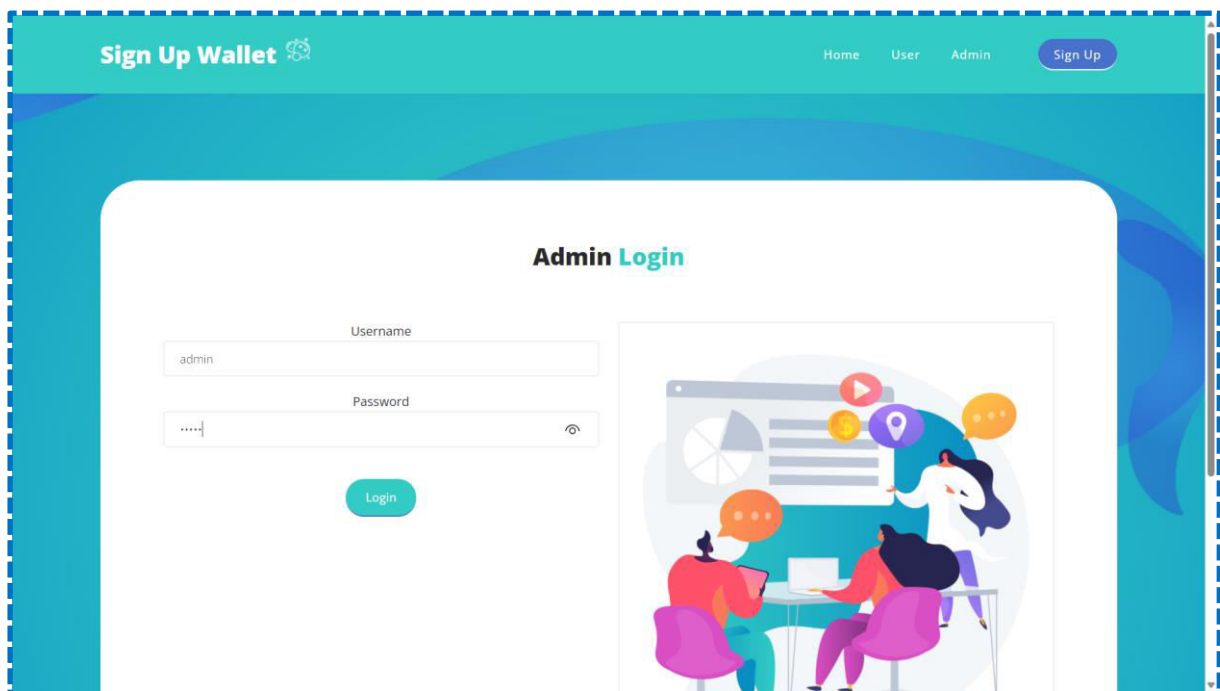


FIG 6: ADMIN LOGIN

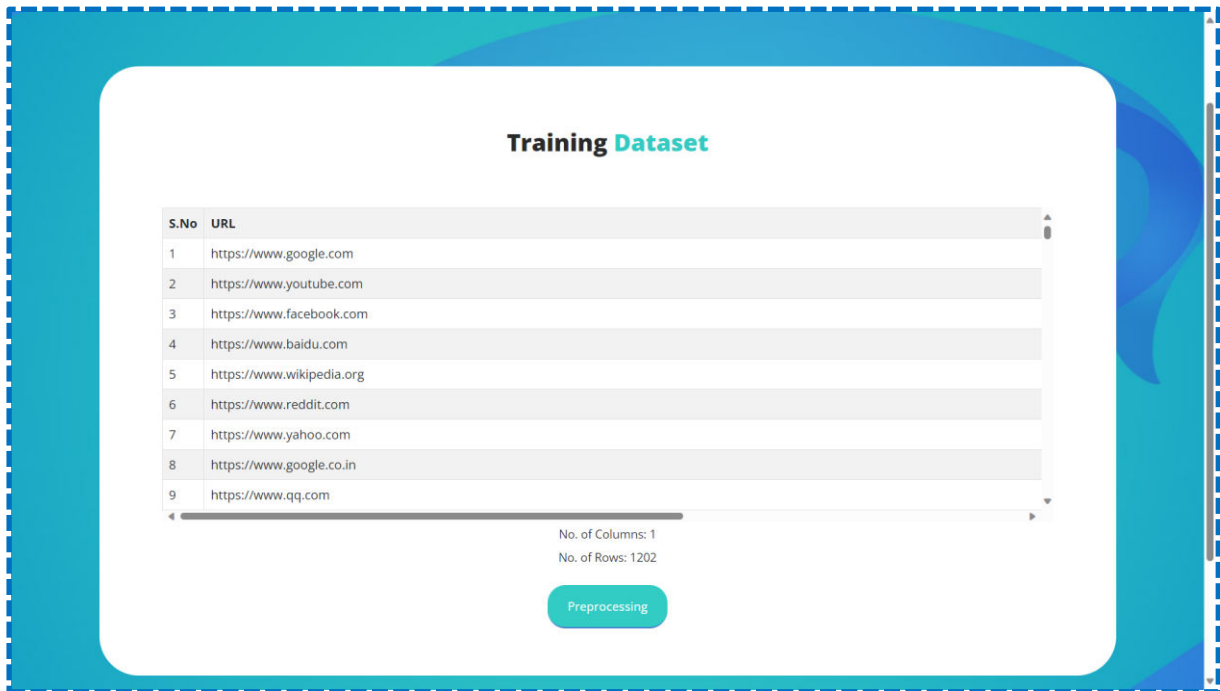


FIG 7: TRAINING DATASET

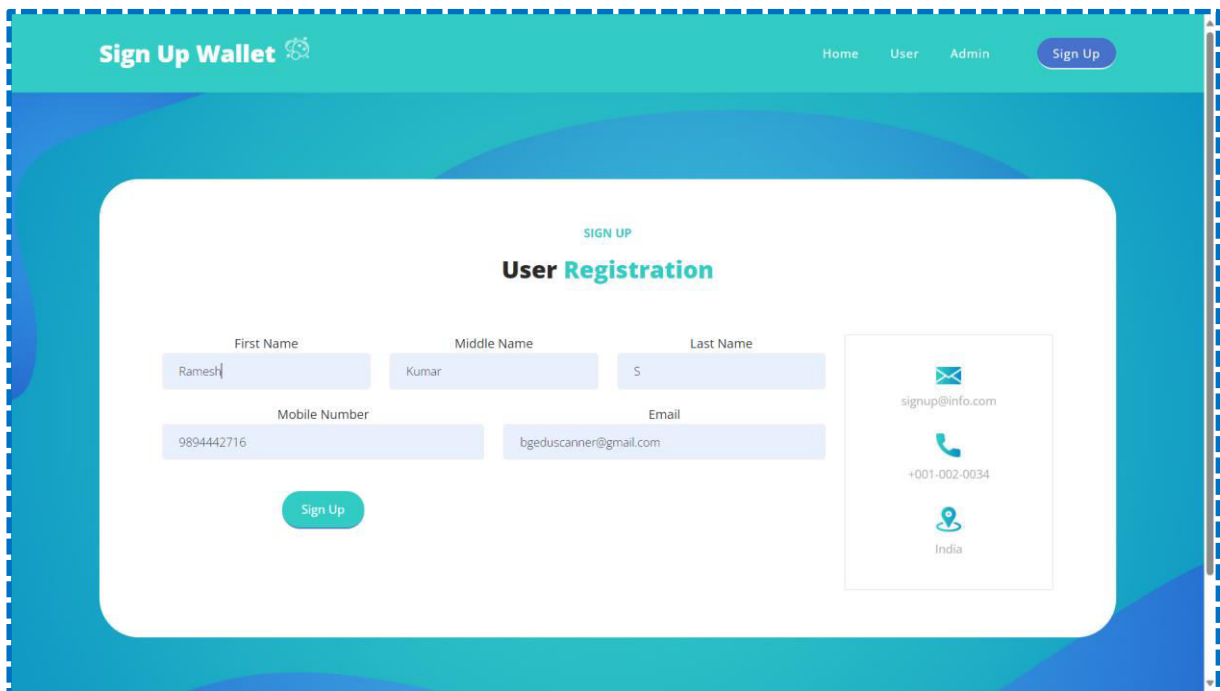


FIG 8: USER REGISTRATION

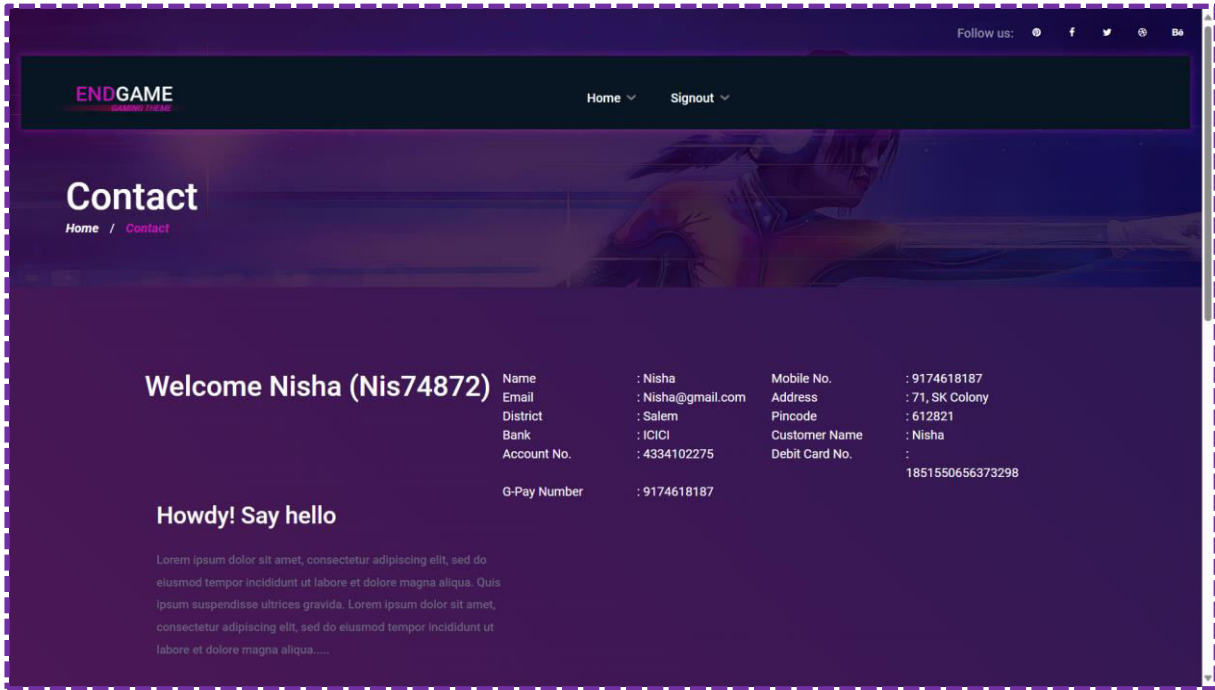


FIG 9: USER DASHBOARD

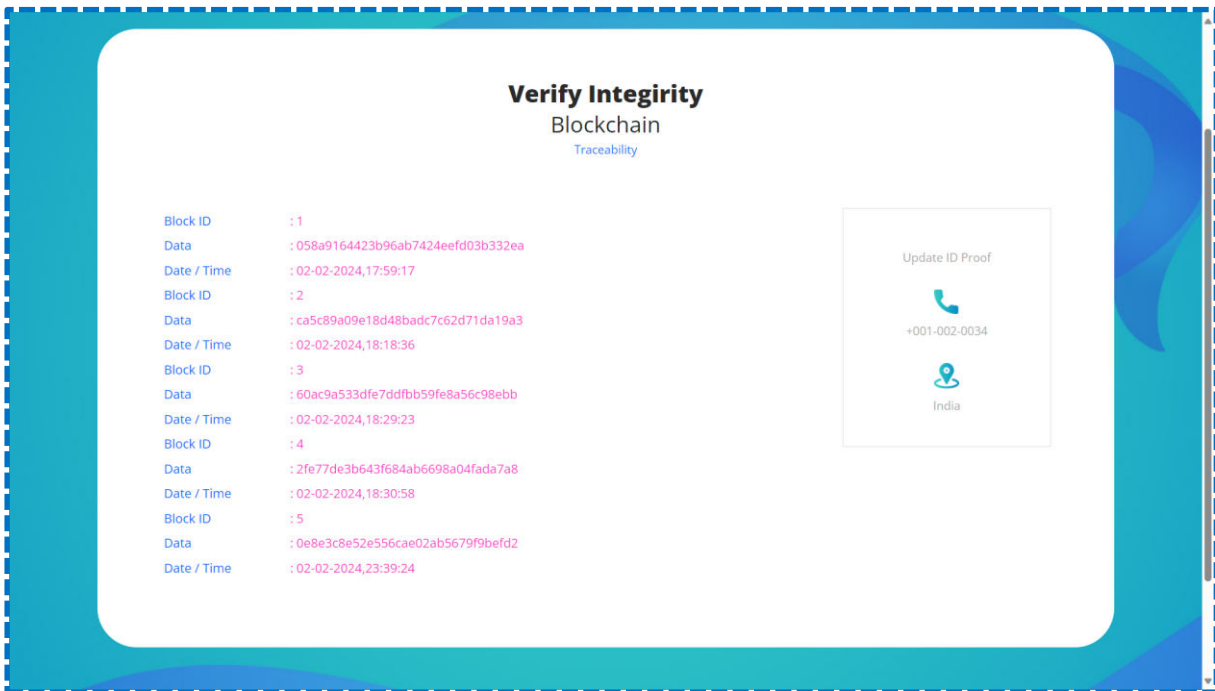


FIG 10: VERIFY INTEGRITY

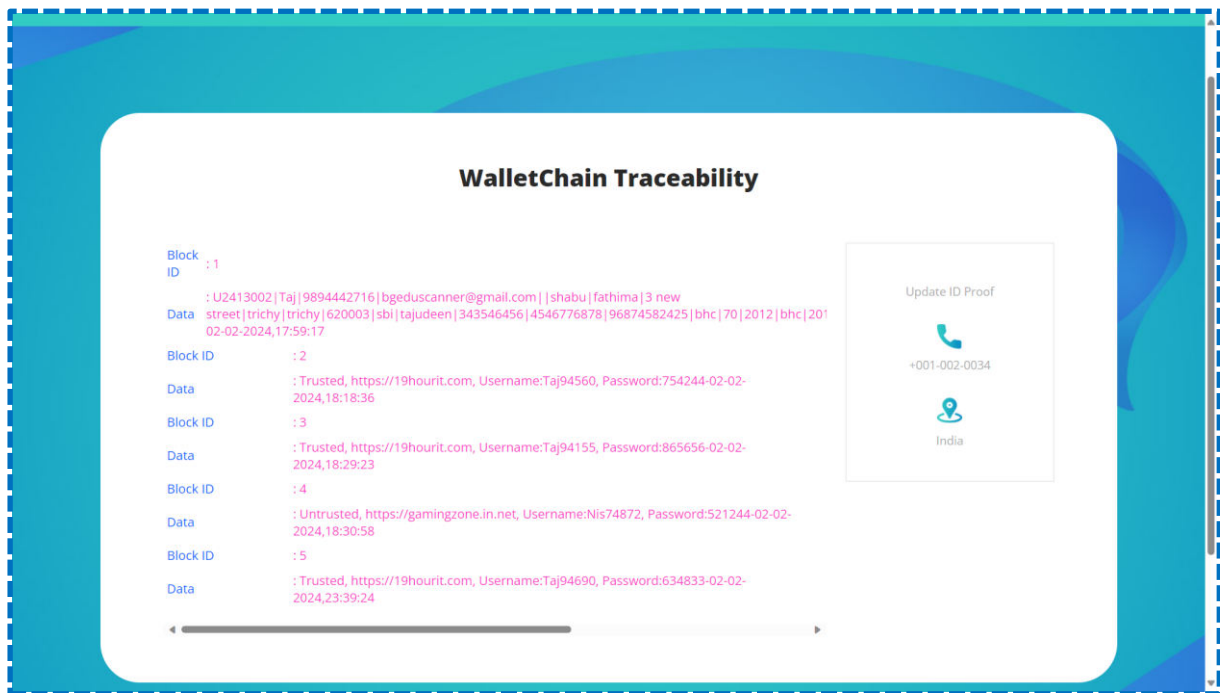


FIG 11: WALLET CHAIN TRACEABILITY

OUTCOMES: The Sign-Up Wallet System has been thoroughly tested and meets the specified requirements. The system demonstrates robust functionality, security, and reliability, ensuring a seamless user experience in managing digital identities and interacting with service providers.

VI.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 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. In conclusion, the Sign-Up Wallet System empowers users with greater control over their digital identities, offering a secure, decentralized, and user-centric approach to digital identity management. This system not only addresses current challenges but also sets a new standard for the future of digital identity ecosystems.

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.
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 self-sovereign 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.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com