WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

PERSONAL INFORMATION PROTECTION IN WALLET SIGNUP USING BLOCKCHAIN AND LOOKUP SUBSTITUTION

K.Praveenkumar [1], #Mr. J.Jayapandian [2]

[1]Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India
[2]M.C.A.,M.Phil.,(Ph.D).,Associate Professor, Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India

ABSTRACT :

Digital identity functions like an online ID, akin to a passport or driver's license, encompassing user attributes. Current systems, which rely on centralized or federated identity management (e.g., Google or Facebook login), are susceptible to large-scale data breaches and unauthorized tracking. These systems fail to safeguard user privacy and do not support the portability of identity data. To tackle these issues, the SignUp Wallet was developed, leveraging blockchain and machine learning for self-sovereign identity management. Users store their digital identity in a wallet with cryptographic keys and utilize a Unique Personal Identifier Code for credential verification. Logistic Regression predicts trusted websites, while a Lookup Substitution Algorithm conceals credentials for untrusted providers, ensuring privacy. This method aims to enhance user control over digital identities, decreasing reliance on centralized systems and mitigating data breach risks.

Keywords: Digital identity, Signup Wallet,Unique Personal Identifier (UPI) Code,Lookup Substitution Algorithm.

INTRODUCTION :

In an era where digital interactions are omnipresent, the protection of Personally Identifiable Information (PII) has become a critical concern for individuals and organizations alike. The increasing frequency and sophistication of data breaches have highlighted the vulnerabilities in current data protection practices, necessitating innovative solutions to secure sensitive information. One such innovation is the Signup Wallet, a blockchain-based system designed to enhance PII security through advanced masking techniques. This system leverages the robust features of blockchain technology to provide a secure, immutable, and transparent framework for managing PII. Blockchain technology, known for its decentralized and tamper-proof nature, offers significant advantages in the realm of data security. By distributing data across a network of nodes, blockchain ensures that no single point of failure can compromise the entire system. This inherent security feature makes blockchain an ideal platform for storing and managing sensitive information such as PII. The Signup Wallet utilizes this technology to create a secure environment where PII is not only protected from unauthorized access but also verifiable and traceable, providing users with confidence in the integrity of their data. At the heart of the Signup Wallet's security mechanism is the concept of PII masking using lookup substitution. This technique involves replacing actual PII with pseudonymous tokens that can be referenced through a secure lookup table. These tokens ensure that even if the data is intercepted or accessed by unauthorized parties, it remains unintelligible without the appropriate decryption key. The use of lookup substitution thus provides an additional layer of security, making it significantly more challenging for malicious actors to extract meaningful information from compromised datasets. The process of PII masking in the Signup Wallet is designed to be both efficient and user-friendly.

LITERATURE SURVEY :

[1] Traditional centralized and federated identity management systems have dominated the digital landscape, where users often depend on centralized authentication servers or identity providers, such as Google or Facebook, to access various services. These systems, however, are inherently vulnerable to large-scale hacks and breaches, and they raise significant privacy concerns due to extensive user data tracking. [2] Self-sovereign identity (SSI), facilitated by blockchain technology, offers a decentralized alternative to conventional identity management systems. This approach eliminates the need for trusted third-party identity providers and grants individuals greater control over their digital identities. Blockchain's immutable ledger and cryptographic features provide a secure basis for managing digital identities without relying on centralized authorities. [3] Machine learning techniques have increasingly been applied in trust evaluation systems to identify trusted service providers in digital environments. Logistic Regression, a widely-used machine learning algorithm, has proven effective in predicting website trustworthiness based on various factors such as domain age, SSL certificate validity, and historical user reviews. By leveraging machine learning, trust evaluation can be automated and adapt to evolving online threats. [4] Privacy-preserving techniques are essential for protecting user data during identity verification processes. Lookup Substitution Algorithms provide a method to mask Personally Identifiable Information (PII) while still allowing for authentication and verification. By replacing sensitive data with pseudonyms or tokens, these algorithms ensure user privacy is maintained, even when interacting with untrusted service providers. [5] The proposed Signup Wallet

integrates blockchain-based self-sovereign identity management with machine learning-driven trust evaluation and privacy-preserving techniques. Users maintain control over their digital identities through cryptographic keys stored in the wallet, while Logistic Regression helps identify trusted service providers. When trust cannot be assured, the system employs a Lookup Substitution Algorithm to generate masked credentials, preserving user privacy during verification processes. By combining these elements, the Signup Wallet project aims to address existing challenges in digital identity management, enhance user control and privacy, and mitigate the risks associated with centralized identity systems and data breaches.

III. PROPOSED SYSTEM :

The proposed system, SignUp Wallet, transforms digital identity management by utilizing blockchain technology and machine learning to boost security and privacy. It introduces self-sovereign identity management, giving users full ownership and control over their digital identities without intermediaries. At its foundation, blockchain technology ensures a decentralized, tamper-proof ledger that provides transparency, immutability, and traceability. The integration of machine learning, particularly Logistic Regression, allows users to assess the trustworthiness of websites, adding an additional security layer. The system offers flexible registration through the SignUp Wallet Web App or Registration API and ensures secure credential verification via a robust process involving a Unique Personal Identifier (UPI) Code. Advanced privacy measures, including a Lookup Substitution Algorithm, protect user data during interactions with untrusted service providers. A Notification Module provides real-time updates, enhancing user experience and transparency. The decentralized ledger improves traceability and accountability, while a user-friendly dashboard offers centralized control over digital identities.

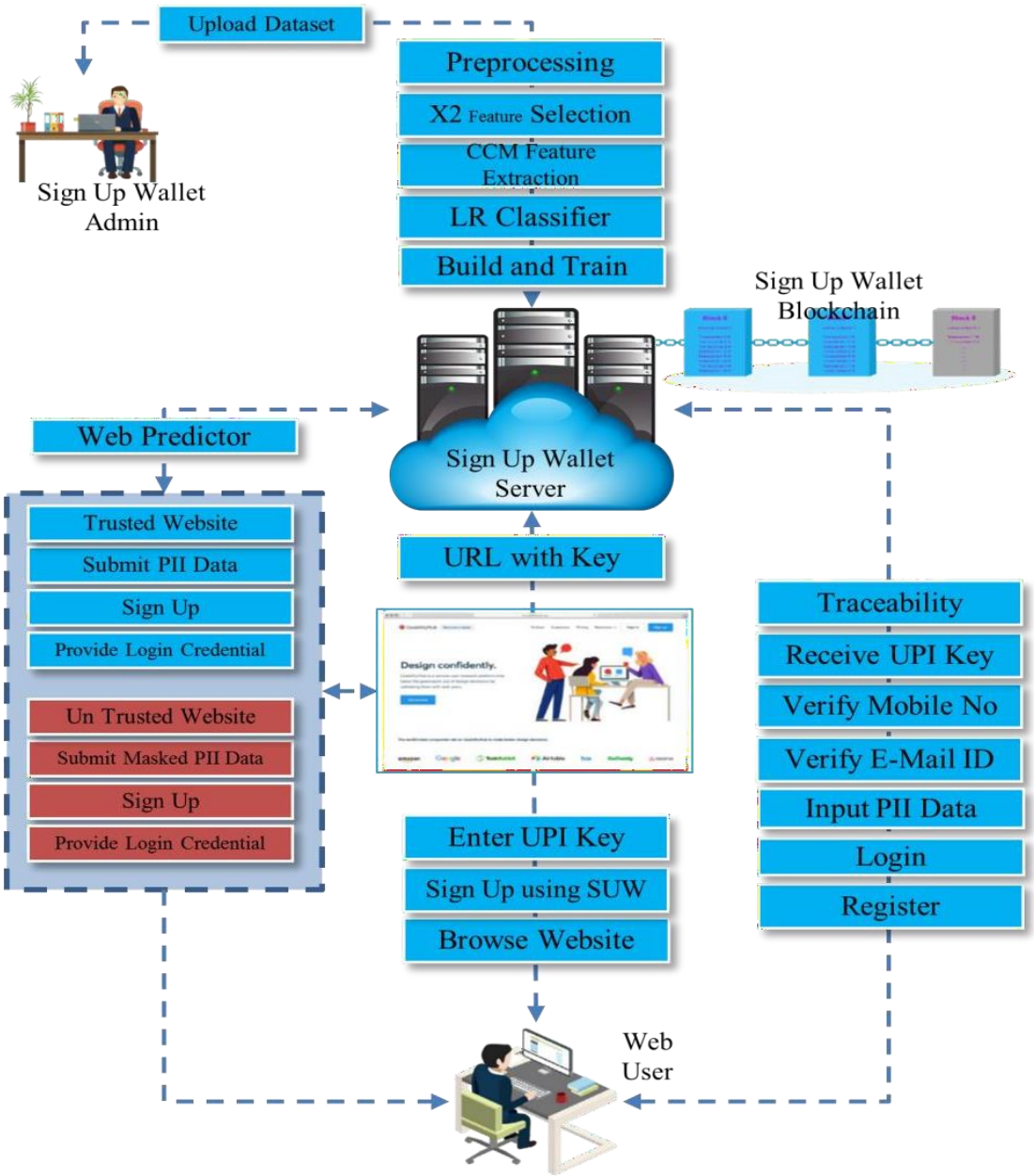


Figure 1: System Architecture of the proposed system

3.1 IMPLEMENTATION

Our project constituted of the below modules,

1.Data Collection

This module centers on collecting a varied dataset of websites, including both trusted and untrusted sites. Web scraping methods are utilized to extract pertinent features and labels for training the model

2.Data Pre-processing

Prior to model training, data undergoes preprocessing. This includes addressing missing values, eliminating duplicates, and transforming categorical variables into an appropriate format. Data normalization and scaling might also be applied to achieve optimal model performance.

3.Feature Selection

A Chi-square test is conducted to identify the most significant features. This module selects features that demonstrate a strong correlation with the target variable, thereby enhancing the model's predictive capability.

4.Feature Extraction

This module entails feature extraction using a Co-occurrence Matrix, which captures the relationships between various features. This technique offers a detailed understanding of the website data, enhancing the model's ability to determine trustworthiness.

5.Model Architecture

In this module, the Logistic Regression model is developed. It includes defining the input layer based on the selected features, configuring the logistic function, and setting up training parameters such as learning rate and regularization.

6.Training

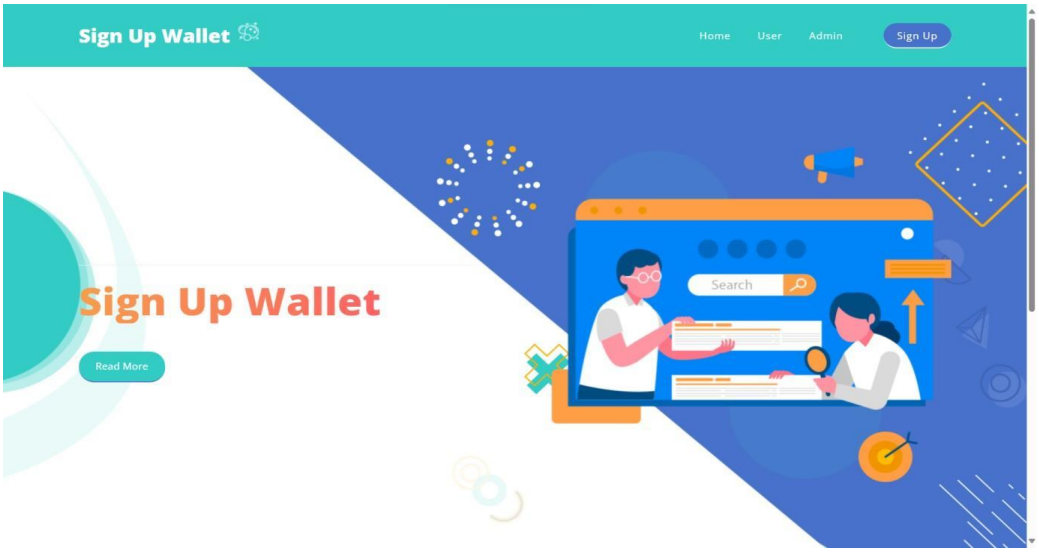
The actual training of the Logistic Regression model occurs in this phase. The model learns to classify websites into trusted (1) and untrusted (0) categories based on the selected and extracted features. Training involves minimizing the logistic loss function to improve predictive accuracy.

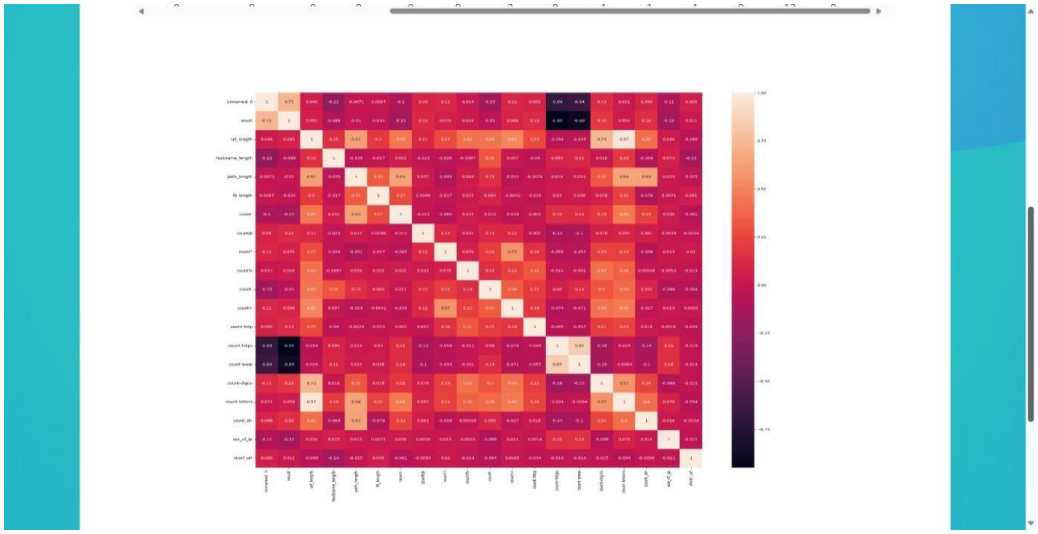
7.Deployment in Wallet Chain

After successful training, the Logistic Regression model is implemented in Wallet Chain, guaranteeing secure and distributed access. This process includes embedding the model into the blockchain environment, facilitating real-time classification of websites within the Wallet Chain ecosystem.

RESULTS AND DISCUSSION :

The testing phase of the SignUp Wallet system demonstrated its efficacy in safeguarding user data while providing seamless digital identity management. Unit testing validated the internal logic of the system, ensuring accurate processing of inputs and outputs. Functional testing confirmed the system's ability to perform as specified, and user acceptance testing (UAT) showed that the system meets end-user requirements for functionality and usability. Integration testing verified that the components and modules of the system interact correctly and adhere to both functional and non-functional requirements. The system's deployment of Logistic Regression for website trust prediction was particularly effective, correctly classifying trusted and untrusted websites, which contributes to the overall security and reliability of the digital identity management process. These comprehensive testing strategies collectively ensured the robustness, reliability, and security of the SignUp Wallet system.





CONCLUSION :

The SignUp Wallet system signifies a major leap in digital identity management by incorporating blockchain technology and machine learning to improve security, privacy, and user control. This decentralized strategy removes the dependence on centralized authorities, thus minimizing the risk of data breaches and unauthorized data tracking. The system's implementation of a Unique Personal Identifier Code simplifies the verification process while ensuring robust security through multi-step verification. For interactions with untrusted service providers, the system utilizes a Lookup Substitution Algorithm to obscure credentials, safeguarding user privacy.

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. Y. Bai, H. Lei, S. Li, H. Gao, J. Li and L. Li,
2. "Decentralized and self-sovereign identity in the era of blockchain: A survey", Proc. IEEE Int. Conf. Blockchain (Blockchain), pp. 500-507, Aug. 2022. K. P. Jørgensen and R. Beck, "Universal wallets", Bus. Inf. Syst. Eng., vol. 64, no. 1, pp. 115- 125, Feb. 2022. Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović and M. Turkanović,
3. "Towards the classification of self-sovereign identity properties", IEEE Access, vol. 10, pp. 88306-88329, 2022. 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. S. Schwalm, D. Albrecht and I. Alamillo, "eIDAS 2.0:
4. Challenges perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI" in Open Identity Summit, Bonn,Germany:GesellschaftfürInformatik, pp. 63-74, 2022.
5. 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. 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.
6. 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.
7. 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.
8. 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. A.Giannopoulou, "Data protection compliance challenges for self-sovereign identity", Proc. 2nd Int. Congr. Blockchain Appl., pp. 91-100, 2020.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.

14. 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.
15. 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.
16. 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.