IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 6, June 2024

Impact Factor: 5.731

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

T. Mukilan[1], P. Kavitha[2], S. Kamalakkannan[3]

PG Student, Department of Computer Applications[1]

Assistant Professor, Department of Computer Applications[2]

Associate Professor, Department of Information Technology[3]

Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

22304252@vistas.ac.in, pkavikamal@gmail.com, kannan.scs@velsuniv.ac.in

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*

Keywords: BlockChain, cryptographic keys, machine learning

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, sign-up forms can be used for generating leads, collecting emails for newsletter, and acquiring new customers. It is a useful tool that can be used across several marketing channels, including social media platforms as well as blogs and websites. Emails are a precious touchpoint that shouldn't be neglected. These are forms aimed at harvesting email addresses to enhance your email list and generate potential leads.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

Product sign-up forms are crucial to e-commerce websites because they're the last barrier before any purchase is made. For product sign-up forms, it's best practice to show the actual product, be very clear, and display security elements to give customer peace of mind.Subscription sign-up forms are a central piece of any subscription-based digital business; it's where the conversions happenService sign-up forms differ from subscription forms as they do not necessarily bind the user through a subscription. Service sign-up forms, like Spotify in the image below, are typically aimed at converting a maximum number of visitors into users. For that to happen, one of the best tools that you can use is a social media sign-up process.

II. LITERATURE SURVEY

MohamedenDieye, Pierre Valiorgue, Self-Sovereign Identities (SSI) using two Zero-Knowledge Proof (ZKP) protocols based on the discrete logarithm difficulty.MortezaAlizadeh, Karl Andersson, OlovSchelén, Focus is on providing users with control over their information and biometrics in a decentralized manner.Comparative analysis of various decentralized identification technologies. The authors survey existing alternatives, particularly self-sovereign identities (SSIs). . These approaches typically leverage blockchain, distributed ledger technology (DLT), zero-knowledge proofs (ZKPs), and other cryptographic techniques to provide individuals with control over their digital identities.

Tao Feng, Pu Yang, Chunyan Liu, Blockchain privacy protection scheme based on zero-knowledge proof to securely.Combine zero-knowledge proof and smart contracts to verify data availability between data owners and cloud service providers while protecting data privacy. A blockchain data privacy protection and sharing scheme based on zero-knowledge proofs (ZKPs) is designed to address the challenge of maintaining confidentiality while sharing sensitive information on a blockchain network.

Tao Feng, Pu Yang, Chunyan Liu,e-wallets as a payment method. The study utilizes the extended Technology Acceptance Model (TAM). Collected 330 data points from e-wallet user's data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). A Blockchain Data Privacy Protection and Sharing Scheme based on Zero-Knowledge Proof (ZKP) is a sophisticated method designed to safeguard sensitive information while enabling secure and transparent data sharing on a blockchain network.

Lukas Stockburger,GeorgiosKokosioulis,AliveluMukkamala, Enhance security and transparency for all stakeholders in the public transportation ecosystem.Analysis of existing public transportation ticketing solutions. Blockchain-enabled decentralized identity management is a novel approach to identity verification and authentication that leverages blockchain technology to provide individuals with greater control, security, and privacy over their personal data.

MdWasiul Karim, e-wallets as a payment method. The study utilizes the extended Technology Acceptance Model (TAM). Collected 330 data points from e-wallet user's data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The ease of accessing and using e-wallets plays a significant role in their adoption among young adults. Factors such as the availability of mobile apps, user-friendly interfaces, and seamless integration with other services influence their convenience

Takemiya and B. Vanieiev,The Sora identity system is designed to offer secure and decentralized identity management leveraging blockchaintechnology.It aims to address issues related to identity theft, fraud, and lack of privacy in traditional identity management systems by providing individuals with self-sovereign control over their digital identities.The system likely utilizes blockchain as the underlying infrastructure to store and manage decentralized identifiers (DIDs) and verifiable credentials securely.

Benarroch, K. Gurkan, R. Kahat, A. Nicolas, and E. Tromer, The proposal likely introduces Zkinterface as a standardized tool or protocol designed to enable interoperability between different implementations of zero-knowledge proof systems.It may address the need for a common interface or format that allows ZKP systems to communicate and interact seamlessly, thereby promoting interoperability and collaboration in the broader zero-knowledge proof ecosystem.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

III. IMPLEMENTATION WORK

The proposal likely introduces an integrative performance framework aimed at providing a comprehensive assessment of higher education students' skills, achievements, and readiness for the labor market. It may utilize distributed ledger technology, such as blockchain, to create a transparent, immutable, and auditable record of students' academic credentials, certifications, work experiences, and other relevant information.

Introduces two ZKP protocols based on the discrete logarithm difficulty and automorphism group properties. This ensures privacy, security, and user autonomy in managing personal data and interactions online. To achieve SSI, various technologies can be employed, including zero-knowledge proofs (ZKPs) and blockchain.Blockchain technology provides a decentralized and immutable ledger where transactions are recorded in a transparent and secure manner. In the context of SSI, blockchain can be utilized to store and manage decentralized identifiers (DIDs) and verifiable credentials. DIDs serve as unique identifiers for individuals, while verifiable credentials contain claims or attributes about the individual (e.g., a university degree or a driver's license). By leveraging block chain, individuals can have full control over their identity-related data, and interactions can be securely recorded and verified without the need for intermediaries.

The document likely presents a comprehensive approach or framework for leveraging digital technologies, such as digital identity, electronic payments, and data sharing, to transform service delivery across various sectors. It may discuss the importance of establishing a digital infrastructure or "stack" that integrates these components to enable efficient, transparent, and inclusive service delivery to citizens and businesses.

IV. EXPERIMENTAL RESULT

Fig.1: Sign Up Wallet

Fig.2: Feature Extraction

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

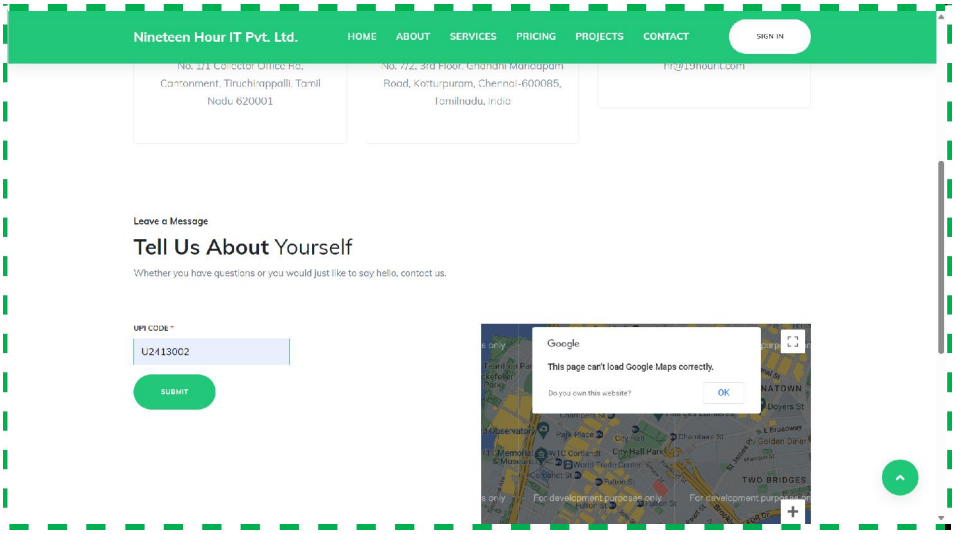

Fig.3: UPI Code

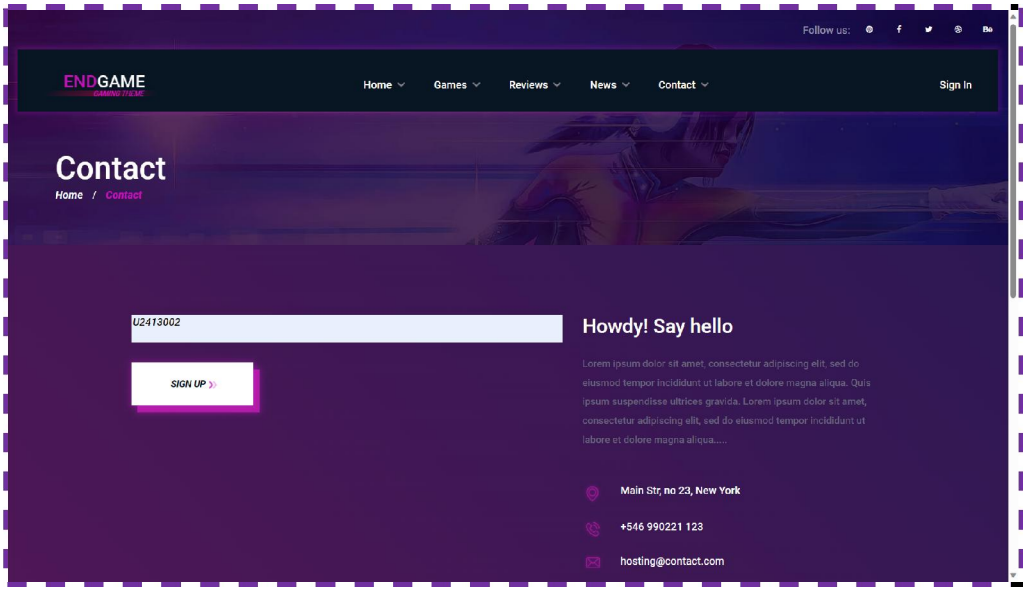

Fig.4: Untrusted

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

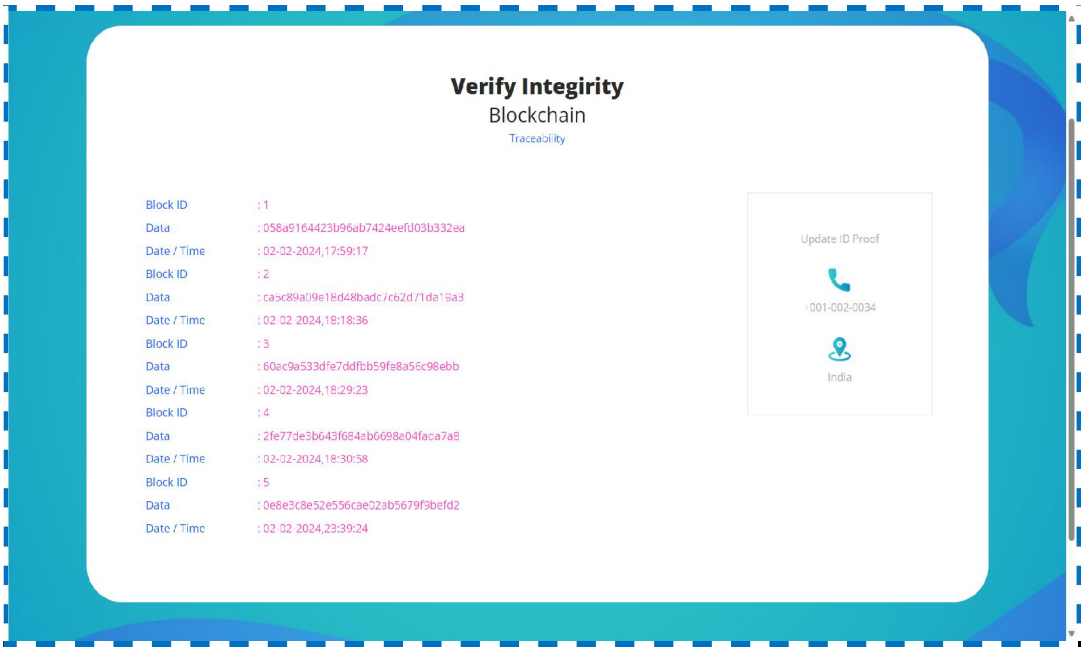

Fig.5: Verify Integrity

V. CONCLUSION

The Sign Up Wallet project introduces a revolutionary approach to digital identity management, leveraging blockchain and machine learning technologies. Addressing the vulnerabilities of centralized identity management, this solution empowers users with control over their digital identities. Users store encrypted data in a secure Sign Up Wallet, utilizing a Unique Personal Identifier (UPI) Code for seamless registration and direct credential verification with trusted service providers. Machine learning, specifically Logistic Regression, enhances security by predicting website trustworthiness. For untrusted providers, a masked credential ensures privacy.This project redefines digital identity management, prioritizing security, privacy, and user autonomy

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:GesellschaftfürInformatik, 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]. 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.