Sign Up Wallet based on Personally Identifiable Information (PII) using Block Chain

[1]Moratanch N, [2]Kanisha G, [3]Kaviya S, [4]Sudha M

[1]*Associate Professor, Adhiyamaan College of Engineering, Hosur.*

[2,3,4] *UG Students, Adhiyamaan College of Engineering, Hosur.*

ABSTRACT

In response to the prevalent concerns surrounding user privacy and the limitations of centralized and federated identity management systems, this research-based project introduces a pioneering Self-Sovereign Identity model that combines blockchain and machine learning technologies. Within this framework, users establish a secure repository for their digital identity within a Sign-Up Wallet, employing a Unique Personal Identifier (UPI) Code for direct credential verification with trusted service providers. The model employs Logistic Regression to assess the trustworthiness of websites. In instances where service providers lack trustworthiness, a masked credential is generated using a Lookup Substitution Algorithm, ensuring privacy throughout the verification process. This innovative approach aims to address the privacy and data portability challenges inherent in existing identity management systems, presenting a promising avenue for enhancing user control and security in the digital world.

Keywords *user privacy, centralized and federated identity, self-sovereign identity model, blockchain, machine learning, secure repository, Sign Up Wallet, Unique Personal Identifier, credential verification, Lookup Substitution algorithm, security.*

1. Introduction

In the rapidly evolving landscape of digital interactions, the management of user identity has become a critical concern, marked by challenges stemming from compromised privacy and limited data portability within conventional centralized and federated models. This research endeavors to pioneer a transformative solution by proposing a Self-Sovereign Identity (SSI) model that integrates blockchain and machine learning methodologies. The primary motivation behind this paradigm shift lies in the urgent need to establish a more secure, privacy-centric, and user-controlled identity management system.

Central to our proposed SSI model is the concept of a Sign-Up Wallet, wherein users can securely store their digital identities. This innovative approach introduces a Unique Personal Identifier (UPI) Code, offering a direct and efficient means for credential verification with trusted service providers. By using blockchain technology, users gain unprecedented control over their identity, mitigating the risks associated with centralized storage and reducing dependency on federated systems.

The application of Logistic Regression further enhances the model's efficacy by predicting the trustworthiness of websites involved in the identity verification process. To address potential concerns regarding untrusted service providers, a sophisticated Lookup Substitution Algorithm comes into play. This algorithm generates masked credentials, ensuring a privacy-preserving mechanism during the verification phase.

In essence, this research-based project envisions a future where users wield greater authority over their digital identities, leading to enhanced privacy, security, and data portability. By bridging the gap between blockchain and machine learning, our proposed SSI model seeks to redefine the standards of identity management systems, promising a more resilient, user-centric, and adaptive framework for the digital age.

2, **Related Works**

[1] Proposing a novel Self-Sovereign Identity (SSI) model, this research introduces two Zero-Knowledge Proof (ZKP) protocols based on discrete logarithm difficulty, addressing data security and decentralization in digital identity systems. The designed SSI protocol ensures minimal information disclosure to trusted parties and complies with eIDAS and GDPR regulations.
[2] This research explores decentralized, privacy-preserving storage systems with incentives, addressing concerns of centralized cloud storage by integrating blockchain and peer-to-peer models. The proposed designs employ cryptographic proofs and anonymous payment mechanisms, presenting a novel approach to incentivize participants and enhance data security.
This paper addresses security and privacy challenges in decentralized smart grid energy trading by proposing a blockchain-based solution with multi-signatures and encrypted messaging streams. The implemented proof-of-concept ensures anonymous negotiation of energy prices and secure trading transactions without relying on trusted third parties, validated through case studies for security analysis and performance evaluation.

[3] Decentralized Identifiers (DID) offer promising solutions for privacy-preserving user identity sharing across diverse services. However, this paper critically examines the security of DID systems, evaluating potential vulnerabilities in data flow and proposing countermeasures for identified threats.
[4] Blockchain's decentralized ledger transforms digital asset transactions but faces scalability, security, and privacy challenges. This paper reviews emerging privacy-preserving solutions, focusing on crypto-privacy techniques, to address issues like anonymity, data control, and compliance in blockchain transactions, particularly within a Self-Sovereign Identity (SSI) framework.
[5] Blockchain technology, propelled by its popularity in cryptocurrency, is revolutionizing healthcare by offering a secure, decentralized framework for managing Electronic Healthcare Records (EHRs). This paper introduces an innovative EHR management system, integrating Blockchain multi-signature stamps and a private channel framework, to enhance data accessibility, security, and patient autonomy in healthcare administration.
[6] In response to the growing importance of transaction anonymity in blockchain, this research categorizes existing privacy protocols based on fundamental building blocks and proposes an evaluation framework considering factors beyond computing resources. Introducing the concept of privacy precision, the study provides a quantifiable measure to assess blockchain privacy efficiency and identifies open research challenges.
[7] 5G's potential in diverse applications like IoT, smart cities, and AR/VR necessitates tailored solutions. This paper proposes a blockchain-based platform for Local 5G operators, addressing challenges in subscriber management, security, and infrastructure.
[8] In the context of rapid societal, economic, and technological advancements, establishing a secure and efficient smart grid architecture is crucial. This paper explores how blockchain technology addresses security and privacy challenges in smart grids, focusing on privacy protection, identity authentication, data aggregation, and electricity pricing for data collection and energy trading processes. Additionally, the study discusses current challenges and outlines future research directions in the realm of smart grids.
[9] The convergence of blockchain (BC) and sixth-generation (6G) networks in augmented reality/virtual reality (AR/VR) applications is a burgeoning area of investigation. This pioneering survey addresses the need for a comprehensive examination of the BC and 6G coalition in the AR/VR space, offering insights into its potential applications, challenges, and an integrative architecture.
[10] This paper explores the advancements in blockchain technology and the growing emphasis on data security, focusing on the research and applications of zero-knowledge proofs. It categorizes and evaluates various protocols, examines their roles in privacy transactions and blockchain scaling, and outlines future trends and improvement directions.
[11] The Internet of Vehicles (IoV) integrates vehicles and their surroundings, facilitating extensive traffic data sharing. Researchers leverage blockchain technology to address resource consumption and safety concerns,
[12] creating a secure and reliable vehicle network with distributed, immutable, and transparent features. Ongoing studies in this domain are summarized, compared, and future trends and opportunities are identified.
[13] This paper explores the formal definition of the IoT-as-a-Service (IoTaaS) business model, emphasizing its potential for cost savings and resource optimization. Addressing technological challenges, it proposes a self-sovereign identity (SSI) solution, aligning with W3C standards and featuring a performance evaluation.
[14] This paper explores the impact of digital transformation on businesses, focusing on Netflix as a case study. Survey results indicate a significant shift towards streaming services, with Netflix emerging as the market leader, driven by its compelling content.
[15] With today’s technological boom, the demand for cloud computing services is increasing day by day. Individuals, companies, and multinational businesses are shifting from self-owned web services to cloud services. Among cloud services providers, the most prominent are Amazon Web Services (AWS), Google Cloud Platform GCP, IBM, and Oracle Cloud.

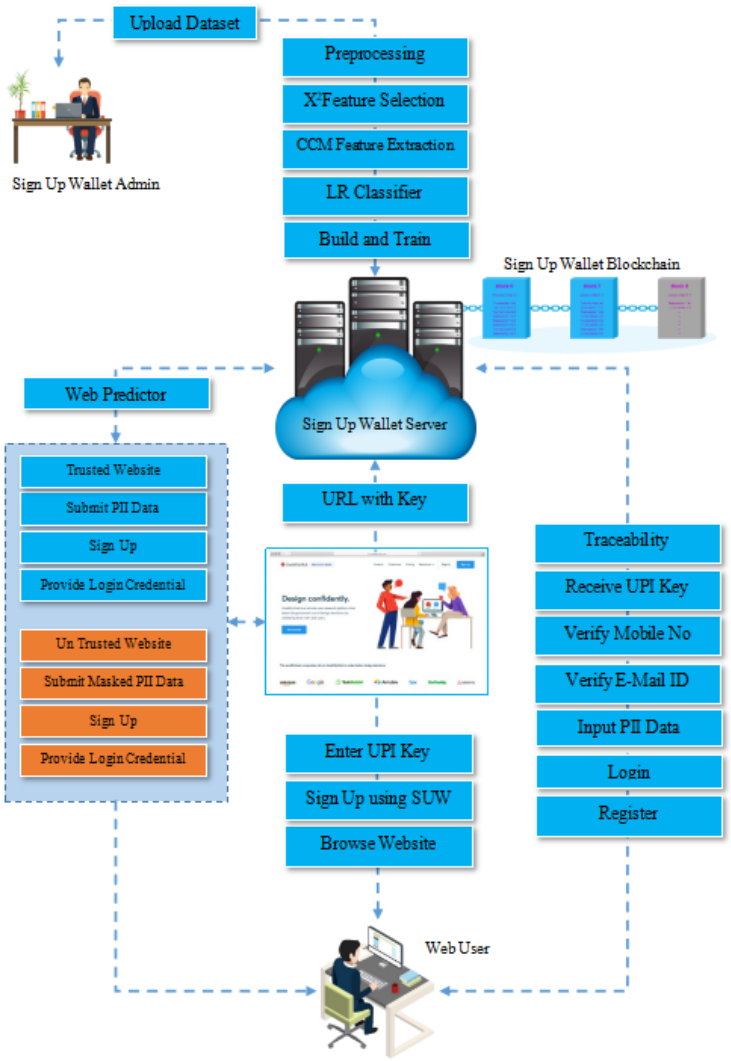


Figure 1*:* System Architecture

3.Architecture Design

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.

The system flow of the Sign-Up Wallet encapsulates a seamless and secure journey for users as they interact with the platform. Below is a detailed overview of the key steps and interactions within the system. Users initiate the process by registering on the Sign-Up Wallet Web App. During registration, users securely input and store their Personal Identifiable Information (PII) in the Wallet Chain. The Wallet Chain utilizes blockchain technology to ensure the immutability and tamper-resistance of the stored data. The system employs a multi-step verification process to ensure user credibility.

Users undergo email verification by clicking on a generated verification link sent to their registered email address. Mobile number verification is conducted through the generation and verification of a One-Time Password (OTP). Upon successful email and mobile verification, the system generates a Unique Personal Identifier (UPI) Code for the user. The UPI Code acts as a unique reference point for the user within the Wallet Chain ecosystem. Users interact with service providers through either the Sign-Up Wallet API, depending on their preference or the platform they are using. Users initiate trust predictions by browsing a website and registering it for prediction using their Sign-Up Wallet API and UPI Key.

The Sign-Up Wallet generates a secure URL incorporating the website name and UPI Key, transferred to the Wallet Chain for verification. The Wallet Chain triggers the trained model to predict the website's trustworthiness, ensuring decentralized and secure predictions. For trusted service providers, the system validates user credentials securely. The process involves UPI Code validation, comprehensive digital identity validation, and granting login access upon successful verification.

Untrusted service providers follow a distinct approach to safeguard user credentials. The system generates a masked credential using a Lookup Substitution Algorithm, ensuring privacy. The masked credential is securely transmitted to untrusted service providers, who validate it without direct access to raw user data. The Notification Module seamlessly integrates with the entire system, providing real-time updates to users on registration, verification, and prediction processes.

All interactions, whether through the web app or API, are recorded in the immutable and timestamped ledger, ensuring traceability and accountability. Users, regardless of their registration method, have access to the user-friendly dashboard for oversight and control over their digital identity.

4.Methodology

Sign Up Wallet serves as a solution for managing digital identities, leveraging blockchain technology and machine learning for enhanced security and privacy. The proposed system, Sign Up Wallet, stands at the forefront of secure, decentralized, and user-centric digital identity management, addressing the shortcomings of traditional identity systems while leveraging the potential of blockchain and machine learning technologies.

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

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 data repositories.

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.

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.

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 Wallet Chain.

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

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.
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. 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.

5.Modules
Sign Up Wallet Web App

The Sign-Up Wallet web application is designed and developed using a robust technology stack consisting of Python, Flask, MySQL, and Bootstrap. It is designed with several key modules to ensure a user-friendly experience in managing digital identities. The User Registration Module allows individuals to create an account, generating a Unique Personal Identifier (UPI) and associated cryptographic keys. Once registered, the Login Module facilitates secure access, for enhanced security. The Dashboard Module serves as a centralized interface, offering users an overview of linked services, credentials, and account activities. Users can manage their personal information and attributes through the Digital Identity Management Module, which supports the addition and verification of various credentials. The Wallet Module securely manages cryptographic keys and enables users to view transaction histories and perform secure transactions, including cryptocurrency transfers. Service Provider Integration facilitates external service linking, while the Trusted Service Provider Prediction Module employs machine learning algorithms to enhance security during the registration process. Credential Verification and Masked Credential Generation Modules ensure secure interactions with service providers, preserving user privacy when needed. 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.

Smart Contract

This module integrates with smart contracts on the Wallet Chain blockchain, enabling advanced functionalities within the Sign-Up Wallet. Users benefit from secure credential issuance and verification through programmable and self-executing smart contracts.

Consensus Algorithm

Critical for transaction validation, the Consensus Algorithm Integration Module integrates with the consensus algorithm of the Wallet Chain blockchain. This guarantees that transactions adhere to established rules, maintaining the integrity of the entire process.

Decentralized Identifier (DID) Management

The PII holder securely stores their digital identity within a Wallet Chain through the Sign-Up Wallet Web App. This specialized digital vault safeguards Personal Identifiable Information (PII) Data, personal attributes, and other pertinent details crucial to the user's identity. The Sign-Up Wallet employs advanced security measures and encryption protocols to ensure the confidentiality and integrity of the stored information.

Verification of E-Mail ID and Mobile Number

For enhanced security and user validation, Wallet Chain initiates a verification process for both the user's E-Mail ID and Mobile Number.

E-Mail Verification

E-Wallet Chain generates an E-Mail verification link, which the user receives in their registered E-Mail ID. By clicking on the link, the user confirms the authenticity of their E-Mail ID.

Mobile Verification

An OTP (One-Time Password) is generated and sent to the user's registered Mobile Number. Successful entry of this OTP verifies the legitimacy of the provided Mobile Number.

UPI Code Generation

Upon successful storage of digital identity, the Wallet Chain generates a Unique Personal Identifier (UPI) Code for the user. This UPI Code serves as a unique and secure identifier, streamlining interactions with various web service providers.

New Way Registration with Web Service Provider

The UPI Code obtained from Wallet Chain facilitates a novel registration approach with web service providers. Users can employ the UPI Code to register securely and seamlessly, introducing a new and efficient way of interacting with online services.

Credential Verification During Registration

Utilizing the UPI Code during the registration process ensures secure and efficient credential verification. The web service provider can verify the user's credentials directly through Wallet Chain, minimizing the need for exposing sensitive information.

Transaction Processing Module

At the core of the integration, the Transaction Processing Module deals the creation and submission of transactions on the Wallet Chain. It ensures the secure execution of every transaction within the Sign-Up Wallet, fostering trust and reliability. Users can review and verify their transaction history directly from the Wallet Chain blockchain, ensuring a high level of transparency and reliability.

Trusted Website Classification: Build and Train

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.

Data Collection

This module focuses on gathering a diverse dataset of websites, incorporating both trusted and untrusted sites. Web scraping techniques are employed to extract relevant features and labels for training the model.

Data Pre-processing

Before model training, data undergoes pre-processing. This involves handling missing values, removing duplicates, and converting categorical variables into a suitable format. Data normalization and scaling may also be applied for optimal model performance.

Feature Selection

To identify the most significant features, a Chi-square test is conducted. This module selects features that exhibit a strong correlation with the target variable, enhancing the model's predictive power.

Feature Extraction

This module involves extracting features using a Co-occurrence Matrix, which captures the relationships between different features. This technique provides a nuanced understanding of the website data, contributing to the model's ability to discern trustworthiness.

Model Architecture

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

Training

The actual training of the Logistic Regression model takes place here. 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 enhance predictive accuracy.

Deployment in Wallet Chain

Upon successful training, the Logistic Regression model is deployed in Wallet Chain, ensuring secure and decentralized access. This involves integrating the model into the blockchain environment, enabling real-time classification of websites within the Wallet Chain ecosystem.

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.

Trusted Website Prediction

This Trusted Website Prediction system involves a seamless process for users to predict the trustworthiness of a website. The integration of Sign-Up Wallet Registration and the trained model in Wallet Chain ensures secure and decentralized predictions. Here's a step-by-step workflow description:

User Input Process

Users initiate the prediction process by browsing a website they want to evaluate for trustworthiness. To register the website for prediction, users utilize their Sign-Up Wallet, providing the Unique Personal Identifier (UPI) Key associated with their digital identity.

URL Generation

The Sign-Up Wallet generates a unique URL incorporating the registered website name and the user's UPI Key. This URL serves as a secure and verifiable reference for the registered website. The generated URL is transferred to the Wallet Chain, ensuring the transaction is recorded and verified in the decentralized blockchain environment.

Prediction

The Wallet Chain triggers the trained model to extract the website name and features using the Co-occurrence Matrix technique. This ensures a nuanced understanding of the website's characteristics. The extracted features are compared with the trained model within the Wallet Chain. The model employs Logistic Regression to predict whether the website is trusted or not based on the learned patterns during training.

Credential Verification and Submission

If the service provider is deemed trusted, this module ensures the secure verification of user credentials. The process involves validating the Unique Personal Identifier (UPI) Code and checking various aspects of the user's digital identity stored in the Wallet Chain. Key functionalities include UPI Code validation, comprehensive digital identity validation, and, upon successful verification, granting the user login access to the trusted service provider.

Masked Credential Generation and Validation

For untrusted service providers, a distinct approach is employed to safeguard user credentials. This module generates a masked credential using a Lookup Substitution Algorithm, ensuring that the original user data remains protected. The functionalities encompass the utilization of a secure algorithm, the generation of a masked credential, and the secure transmission of this masked credential to the untrusted service provider. This module facilitates the validation of the masked credential by untrusted service providers without direct access to the user's

original credentials. It involves receiving the masked credential, applying the Lookup Substitution Algorithm for decryption or transformation, and validating the decrypted credential without exposing the raw user data. The process ensures a secure and privacy-preserving verification for untrusted service providers and provide login credential to access the untrusted service provider

User Dashboard

Sign Up Wallet Admin Dashboard

Login

The admin accesses the Sign-Up Wallet Admin Dashboard by securely logging in with authorized credentials, ensuring exclusive access to administrative functionalities.

Train the Model

Within the admin dashboard, there is a dedicated module for training the trusted website predictor model. This involves updating the machine learning model with new data, enhancing its accuracy and adaptability over time.

User Management

The admin oversees user management, enabling tasks such as adding new users, modifying user privileges, or deactivating accounts. This ensures efficient control over the user ecosystem.

System Maintenance

The admin has access to system maintenance features, facilitating tasks like updating software, managing security protocols, and ensuring the overall health of the Sign-Up Wallet system.

User Dashboard

Register with Sign Up Wallet Web App

Users initiate their interaction by registering with the Sign-Up Wallet Web App. This involves creating an account and providing necessary information for digital identity management.

Login to Sign Up Wallet Web App

Users securely log in to their Sign-Up Wallet Web App accounts using authenticated credentials, ensuring a protected access point to their digital identity.

Store PII Data in Wallet Chain

Upon login, users have the capability to store their Personal Identifiable Information (PII) securely in the Wallet Chain, leveraging blockchain technology for enhanced security.

Receive UPI Code

The system generates a Unique Personal Identifier (UPI) Code for each user, serving as a unique reference point for their digital identity within the Sign-Up Wallet ecosystem.

Register Other Websites with Sign Up Wallet Registration API using UPI Code

Users can register additional websites with the Sign-Up Wallet Registration API by providing the UPI Code. This seamless process ensures a secure and streamlined registration experience.

Receive Login Credential to Access the Website

After successful registration, users receive login credentials specific to the registered website, enabling secure access without the need to expose their raw data

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. Administrators benefit from a centralized view, enabling oversight and compliance monitoring. Integrated with the Notification Module, users receive real-time updates, creating a seamless and informed user journey. This tamper-resistant traceability log builds trust, enhances security, and provides a comprehensive record of digital identity interactions.

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.

Consensus algorithm

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

To accommodate this reality, consensus algorithms necessarily assume that some processes and systems will be unavailable and that some communications will be lost.

Applications of consensus algorithms include:

Deciding whether to commit a distributed transaction to a database. Designating node as a leader for some distributed tasks. Synchronizing state machine replicas and ensuring consistency among them.

Consensus algorithms support many real-world systems including Google's PageRank, load balancing, smart grids, clock synchronization and drone control. In Blockchain networks, the three main kinds of consensus algorithms for arriving at consensus in a distributed manner are Proof of Work (POW), Proof of Stake (POS), and Practical Byzantine Fault Tolerance (PBFT).

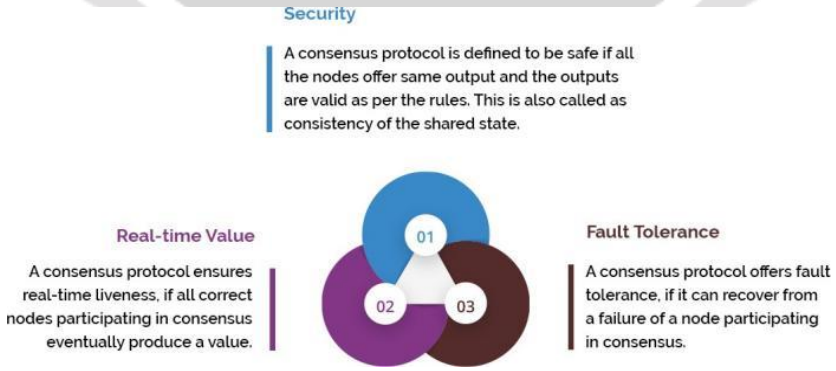


Figure 2*:* Consensus algorithm

6.RESULTS

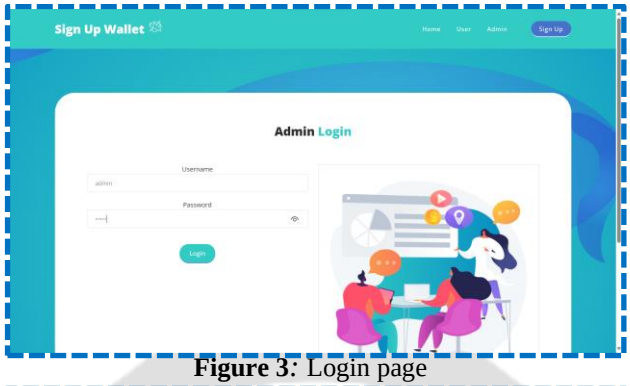


Figure 3*:* Login page

Figure 4*:* Training Dataset

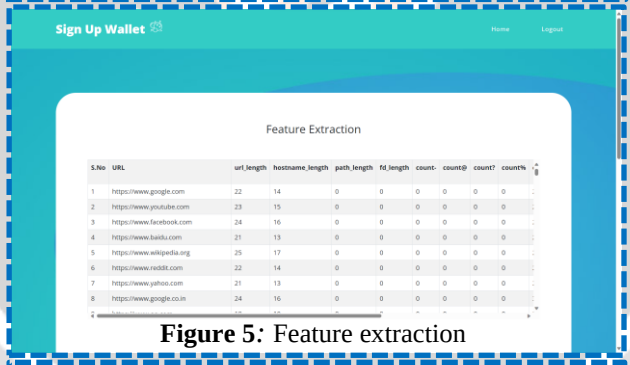


Figure 5*:* Feature extraction

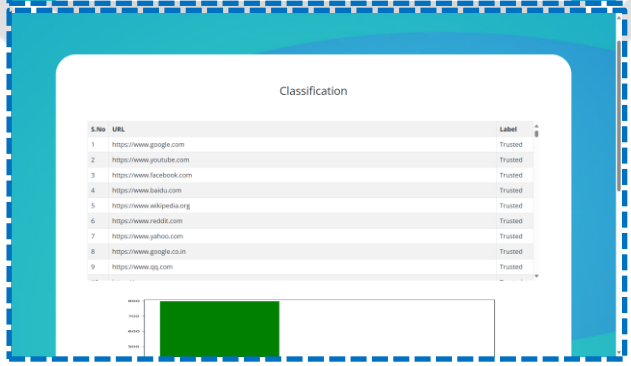


Figure 6*:* Classification

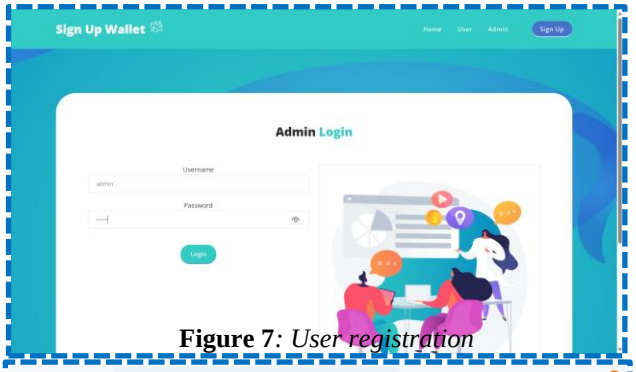


Figure 7*: User registration*

Figure 8: E-mail verification

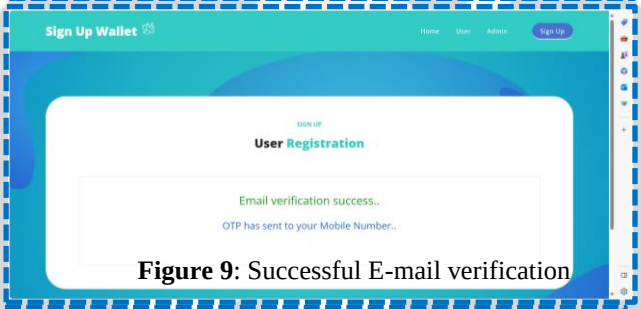
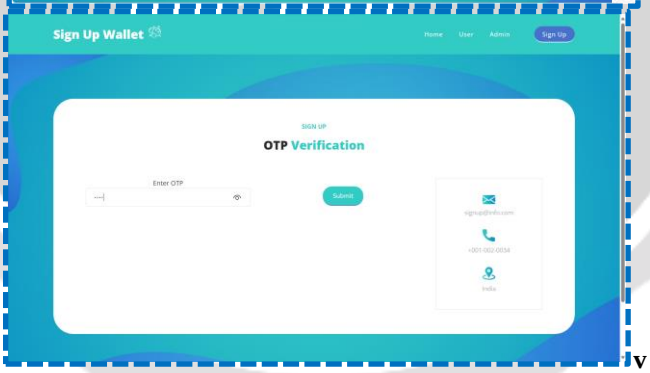


Figure 9: Successful E-mail verification



v

Figure 10: OTP verification

Figure 11: User registration

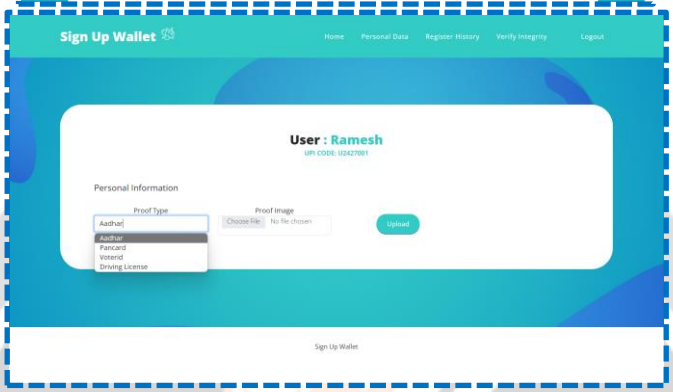


Figure 12: User registration with details

7. 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.

8.Acknowledgement

I would like to express my heartfelt gratitude to all those who contributed to the successful completion of the Seminar Hall Booking Management System project. First and foremost, I extend my sincere thanks to our project supervisor, Dr. Moratanch N for their unwavering support, guidance, and valuable insights throughout the entire development process. I am deeply appreciative of the Head of our Department, Dr. G. Fathima, faculty members and staff who provided their expertise and resources, enriching the project with their knowledge. Special thanks to my fellow teammates for their collaborative spirit, dedication, and hard work, which played a pivotal role in achieving our shared goals. I am also thankful to the academic institution for fostering an environment that encourages innovation and continuous improvement. Lastly, I extend my gratitude to friends and family for their understanding and encouragement during the project's journey. Each contribution, no matter how small, has been instrumental in making this project a success.

9. References

[1] mohameden dieye, pierre valiorgue, jean-patrick gelas, el-hacen diallo, parisa ghodous, frédérique biennier, and éric peyrol, date of publication 20 April 2023, date of current version 24 May 2023. DOI: 10.1109/ACCESS.2023.3268768.

[2] Kopp, Henning Johannes Gustav, A privacy-preserving decentralized storage with payments based on a blockchain, Institut für Verteilte Systeme, doi : http://dx.doi.org/10.18725/OPARU-15013.

[3] Nurzhan Zhumabekuly Aitzhan, Davor Svetinovic, Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams, Published in: IEEE Transactions on Dependable and Secure Computing (Volume: 15, Issue
[4] Bong Gon Kim; Young-Seob Cho; Seok-Hyun Kim; Hyoungshick Kim; Simon S. Woo, A Security Analysis of Blockchain-Based Did Services, Page(s): 22894 - 22913, Date of Publication: 27 January 2021, Electronic ISSN: 2169-3536, DOI: 10.1109/ACCESS.2021.3054887.
[5] Jorge Bernal Bernabe; Jose Luis Canovas; Jose L. Hernandez-Ramos; Rafael Torres Moreno, Privacy-Preserving Solutions for Blockchain: Review and Challenges, Page(s): 164908 - 164940, Date of Publication: 31 October 2019, Electronic ISSN: 2169-3536, DOI: 10.
[6] Susmita Mondal, Mehak Shafi, Sumeet Gupta, and Sachin Kumar Gupta, Blockchain Based Secure Architecture for Electronic Healthcare Record Management, S. Mondal et al. / GMSARN International Journal 16 (2022) 413-426.
[7] Aisha Zahid Junejo,ORCID, Manzoor Ahmed Hashmani, ORCID and Mehak Maqbool Memon, Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges, https://doi.org/10.3390/app11157013, Submission received: 8 July 2021 / Revised:
[8] Nisita Weerasinghe; Tharaka Hewa; Madhusanka Liyanage; Salil S. Kanhere; Mika Ylianttila, A Novel Blockchain-as-a-Service (BaaS) Platform for Local 5G Operators, ublished in: IEEE Open Journal of the Communications Society (Volume: 2), Page(s): 575 - 601,
[9] Ya-Nan Cao a, Yujue Wang b, Yong Ding a c, Zhenwei Guo b, Qianhong Wu d, Hai Liang a, Blockchain-empowered security and privacy protection technologies for smart grid, Computer Standards & Interfaces, Volume 85, April 2023, 103708.
[10] Pronaya Bhattacharya; Deepti Saraswat; Amit Dave; Mohak Acharya; Sudeep Tanwar; Gulshan Sharma, Coalition of 6G and Blockchain in AR/VR Space: Challenges and Future Directions, Published in: IEEE Access (Volume: 9), Page(s): 168455 - 168484, Date of Publi.
[11] Yu Zhou, Zeming Wei, Shansi Ma & Hua Tang, Overview of Zero-Knowledge Proof and Its Applications in Blockchain, Conference paper, First Online: 16 December 2022, Part of the Communications in Computer and Information Science book series (CCIS,volume 1736).
[12] Junting Gao, Chunrong Peng 2,Tsutomu Yoshinaga 1,Guorong Han 3,Siri Guleng 4 andCelimuge Wu 1, Blockchain-Enabled Internet of Vehicles Applications, Submission received: 6 February 2023 / Revised: 28 February 2023 / Accepted: 8 March 2023 / Published: 11 M.
[13] Santiago de Diego; Cristina Regueiro; Gabriel Maciá-Fernández, Enabling Identity for the IoT-as-a-Service Business Model, Published in: IEEE Access (Volume: 9), Page(s): 159965 - 159975, Date of Publication: 25 November 2021, Electronic ISSN: 2169-3536, D
[14] Manuel Au-Yong-Oliveira, Miguel Marinheiro & João A. Costa Tavares, The Power of Digitalization: The Netflix Story, World Conference on Information Systems and Technologies, First Online: 18 May 2020.
[15] Osama Mustafa, Overview of Amazon Web Services, A Complete Guide to DevOps with AWS pp 1–35.