IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305146 |

Implementation of Sign up Wallet Revolutionizing Digital Identity Management with Blockchain and Machine Learning

[1]Mr. R. Kumaran, [2]R. Pooja Sri, [3]G. Silviya,[4]S.Thirisha

[1]Professor, Dept. of IT, P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, India

[2,3,4] UG Student, Dept. of IT, P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, 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.

KEYWORDS*:* Machine learning, Blockchain, suspicious website, secured Digital Identity, Lookup substitution

I. INTRODUCTION

A. Overview

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. The problem is that a lot of businesses do not bother to optimize their sign-up forms for conversion. Sign-up forms are still very valuable in generating leads for business in 2020. A sign-up 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

B. Objective

The aim of the project is to revolutionize digital identity management by introducing a secure, decentralized, and user-centric approach. The project seeks to address the limitations of existing centralized and federated systems, empowering individuals with greater control over their digital identities while enhancing security and privacy.

EXISTING SYSTEMS AND PROPOSED SYSTEMS

C. Existing systems

3) ages online with ease.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

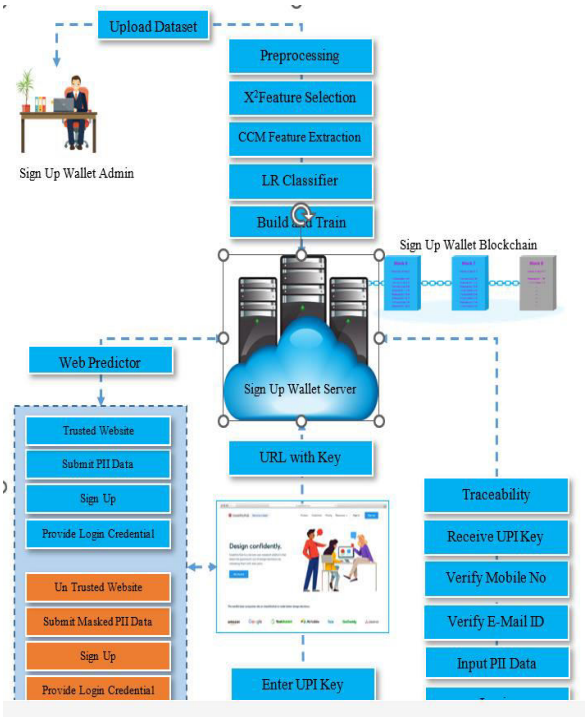
|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305146 |

II. EXISTING SYSTEMS AND PROPOSED SYSTEMS

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. The centralized storage of user data makes it a target for large-scale hacks and data breaches, putting users at risk of identity theft and other malicious activities. 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. At its core, the E-wallet architecture employs a distributed ledger, ensuring that transaction records are securely maintained across a network of nodes. This decentralized nature adds an extra layer of security, making the system resistant to tampering and unauthorized alterations. Elliptic Curve Digital Signature Algorithm The Elliptic Curve Digital Signature Algorithm (ECDSA) is a prominent asymmetric cryptographic algorithm designed for digital signatures, offering a high level of security with relatively shorter key lengths compared to alternative algorithms. Its security foundation is rooted in the mathematical properties of elliptic curves over finite fields. The algorithm involves the use of a private key known only to the entity generating the signature and a corresponding public key, which is openly shared and used for signature verification. ECDSA's 4 signature generation process incorporates intricate mathematical operations on elliptic curves, producing a unique digital signature for the signed data. RSA The Rivest–Shamir–Adleman (RSA) algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, stands as a cornerstone in the realm of asymmetric cryptography. Primarily designed for secure data transmission and digital signatures, RSA relies on the mathematical complexity of factoring large composite numbers. The key components of RSA involve a pair of keys—a public key for encryption, open to anyone, and a private key for decryption, kept confidential. Key generation in RSA entails the selection of two large prime numbers, and encryption is achieved by encrypting the message with the recipient's public key, ensuring that only the possessor of the corresponding private key can decrypt the message.

A. ARCHITECTURE DESIGN



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305146 |

B. MODULES

There are 7 modules following,

1. Sign Up Wallet Web App
2. Wallet Chain Integration
3. Trusted Website Classification: Build and Train
4. Sign Up Wallet Registration API
5. User Dashboard
6. Wallet Chain Traceability
7. Notification

C. Module DESCRIPTION

a) **Sign Up Wallet Web App**

b) Users can manage their personal information and attributes through the Digital Identity Management Module, which supports the addition and verification of various credentials.

c) **2. Wallet Chain Integration:**

d) 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.

e) **3. Trusted Website Classification: Build and Train:**

f) 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.

III. SYSTEM SPECIFICATION

Hardware Requirements

- Operating System: Windows 10 or higher
- Python: Version 3.7 or higher
- Flask: Version 2.0 or higher
- MySQL: Version 8.0 or higher
- Python Packages: Numpy, Pandas, Matplotlib, and Scikit-learn
- Web Server: Apache Web Server (in WampServer)

What is Python 3.7.4

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. Python is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain

. • Machine Learning

• GUI Applications (like Kivy, Tkinter, PyQt etc.)

• Web frameworks like Django (used by YouTube, Instagram, Dropbox)

• Image processing (like OpenCV, Pillow)

• Text processing and many more.

What is MySQL

MySQL is currently the most popular database management system software used for managing the relational database. It is open-source database software, which is supported by Oracle Company. It is fast, scalable, and easy to use database management system in comparison with Microsoft SQL Server and Oracle Database 6.4 Why we use Wampserver WampServer is a Windows web development environment. It allows you to create web applications with Apache2, PHP and a MySQL database. Alongside, PhpMyAdmin allows you to manage easily your database. WampServer is a reliable web development software 20 program that lets you create web apps with MYSQL database and PHP Apache2. With an intuitive interface, the application features numerous functionalities and makes it the preferred choice of developers from around the world. The software is free to use and doesn't require a payment or subscription.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305146 |

Why we use Bootstrap 4

Bootstrap is a free and open-source tool collection for creating responsive websites and web applications. It is the most popular HTML, CSS, and JavaScript framework for developing responsive, mobile-first websites. It solves many problems which we had once, one of which is the cross-browser compatibility issue. Nowadays, the websites are perfect for all the browsers (IE, Firefox, and Chrome) and for all sizes of screens (Desktop, Tablets, Phablets, and Phones).

What is Flask

Flask is a web framework. This means flask provides you with tools, libraries and technologies that allow you to build a web application. This web application can be some web pages, a blog, a wiki or go as big as a web-based calendar application or a commercial website. Flask is often referred to as a micro framework. It aims to keep the core of an application simple yet extensible. Flask does not have built-in abstraction layer for database handling, nor does it have formed a validation support. Instead, Flask supports the extensions to add such functionality to the application.

What is Blockchain

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. 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 impossibleextremely 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.

What is 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. tasets to train its algorithms

IV. 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 WalletChain, 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 WalletChain 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.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305146 |

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.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details