Block Chain Based Personal Identity Security System

Nandhini V, Ponshivani S, Priyadarshini P
Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore

Abstract-The SHA-256 based Block chain Based Personal Identity Security System offers a strong, decentralized answer to the growing problems with identity theft. This system uses the SHA-256 cryptographic hash function to enable tamper-resistant storage and retrieval of identification information, using the power of block chain technology. Since the SHA-256 algorithm is irreversible, it essentially eliminates the possibility of unwanted changes, improving security and ensuring data integrity. The system reduces the possibility of illegal access and single points of failure by decentralizing identity management. In an increasingly digital and linked world, users are able to protect their identity with resilience by having control over their personal data and reaping the benefits of an immutable and transparent ledger.

Keywords: Blockchain, Personal Identity, Cyber Threats

1. INTRODUCTION

The adoption of a block chain-based personal identity security system is a novel way to overcome the weaknesses in conventional identity management systems at a time of fast digitization and growing cyber threats. By using the decentralized and unchangeable characteristics of block chain technology, this inventive approach guarantees improved security, confidentiality, and accuracy of personal data. People may take unprecedented control over their digital identities by using cryptographic principles and decentralizing identity data over a network of nodes. This reduces the possibility of identity theft, illegal access, and data breaches. Personal identity management will become more robust and user-centric as a result of blockchain's transparent and tamper-resistant features, which also strengthen authentication and foster confidence in the digital ecosystem.

1.1 BLOCKCHAIN

Block chain is a revolutionary technology that became well-known with the emergence of cryptocurrencies. It is a distributed and decentralized ledger system with broad applications in a number of sectors. Block chain is essentially a transparent and safe digital ledger that records and verifies transactions via a network of linked nodes. Block chain is unique in that each connected block of data is cryptographically protected, preventing fraud and manipulation. This immutability makes the system unique. Because the technology is decentralized, there is no need for middlemen, which promotes participant confidence and lowers the possibility of data manipulation. Block chain is becoming more widely acknowledged for its potential to improve security, efficiency, and transparency in a variety of industries beyond finance, including as supply chain management and the healthcare industry. As a cornerstone of the decentralized digital future, block chain keeps redefining the ways in which data is exchanged, stored, and verified in the rapidly changing digital world.

1.2 PERSONAL IDENTITY

A complex concept at the nexus of uniqueness and social recognition, personal identity includes all of the distinctive qualities and traits that make each person unique. It extends beyond the material parts of life into the domain of individual experiences, convictions, and connections that form a unique sense of self. Digital footprints and online profiles are all part of the personal identity that permeates the modern digital world. The notion of personal identification is becoming more and more entwined with privacy, security, and ethical concerns of data management as technology continues to change our interactions and lives. The study of personal identity explores philosophical, psychological, and technical aspects while striking a careful balance between the need to protect one's identity in a linked world and the need for self-expression. This highlights the changing character of human identity in the contemporary day.

1.3 CYBER THREATS

The prevalence of cyber risks has grown to be a significant problem in our technologically advanced and linked society, clouding the digital environment. Cyber threats are any number of malevolent actions carried out with the intention of jeopardizing the availability, confidentiality, or integrity of digital

information by people, organizations, or even nation-states. These threats, which may range from complex hacking efforts to more typical phishing scams and malware assaults, take advantage of weaknesses in computer networks, human habits, and computer systems. Cybercriminals' tactics also evolve with technology, therefore it is critical for people, companies, and governments to continually improve their digital defences with vigilance and proactivity. The dynamic character of cyber threats highlights how crucial cybersecurity measures are to maintaining the privacy of sensitive and personal data, the dependability of vital infrastructure, and public confidence in our networked digital environment.

2. LITERATURE REVIEW

2.1 BLOCKCHAIN-BASED IDENTITY VERIFICATION SYSTEM

In this article, Arshad Jamal et al. have proposed It is a bother to constantly present physical papers for each registration procedure. In addition, the procedure is prolonged in the event that they are misplaced, and if those papers are accessed by unauthorized individuals, it will facilitate identity theft. Thus, the goal of this article is to create a decentralized system that is akin to the blockchain idea so that anyone who have registered may access the personal information of users. To put it another way, three consumers are intended to utilize this system: users, authorities, and third parties (requesters). Most systems these days are vulnerable to significant data breaches. Nonetheless, other studies—such as one that utilizes the real-world example of Aadhaar—have postulated that block chain technology could be able to alleviate this issue. In summary, this research strengthens the idea that blockchain identification is essential to enabling people to take ownership of their personal information. People's personal identities should be digitalized on the block chain as well, as the majority of research is concentrated on the blockchain-based storage systems used by enterprises. There would be more confidence that the data is authentic and trustworthy if the identity verification system is fully controlled by the person. Identity theft is a crime that affects a large number of individuals, particularly in recent years, and the number of victims rises annually. Identity theft is the illegal access to someone's personal information. In the United States alone in 2017, one in fifteen persons were estimated by Javelin Strategy & Research to be at risk of being victims of identity theft. Thus, it would be very advantageous to have a system that allows users to monitor access to personal information. In relation to blockchain-based identity management.

2.2 BPDIMS: A BLOCKCHAIN-BASED PERSONAL DATA AND IDENTITY MANAGEMENT SYSTEM

In this work, Benedict Faber et al. have suggested Concerns about the technological, commercial, and ethical elements of user data privacy and security have been raised by recent incidents involving the misuse of personal information obtained from social media platforms and many breaches of user identification data. One of the biggest improvements to data privacy law in recent memory is the European Union's General Data Protection Regulation (GDPR), which includes a number of important legal requirements for data controllers and processors in order to empower and safeguard the privacy of EU residents. Our study presents a high-level architectural and conceptual design for a human-centric, GDPR-compliant personal data and identity management system based on blockchain technology: the Blockchain-based Personal Data and Identity Management System (BPDIMS). We explain how blockchain technology is used in the design of BPDIMS to provide a high degree of security, trust, and transparency. We talk about how BPDIM's human-centric approach to GDPR compliance gives end users more control over their personal data and improves their empowerment. Both our lives and the copious amounts of personal data trails we leave behind have grown more computerized. Currently, the bulk of revenues are made by a small number of very big multinational firms which charge customers for services that they utilize their data for. Although data analytics may provide customers improved services, individuals no longer have as much control or oversight over their personal information. Concerns about the technological, economic, political, and ethical elements of personal data have also been brought up by the recent Cambridge Analytica incident, which included the misuse of users' personal information from Facebook to influence votes in the US Elections 20161.For first authorship, all three of the writers contributed equally. gathering and evaluation by third parties and platform owners like Facebook Users now lack information about which services are processing their personal data, why, and whether or not they are giving their data to third-party providers without their knowledge.

2.3 PERSONAL ARCHIVE SERVICE SYSTEM USING BLOCKCHAIN TECHNOLOGY: CASE STUDY, PROMISING AND CHALLENGING

In this research, Yixuan Zhu et al. have proposed Blockchain is an ever-expanding collection of records, or blocks, connected and safeguarded by encryption. A timestamp, transaction data, and a hash pointer serving as a link to a previous block are normally included in every block. Blockchains are by their very nature resistant to data alteration. The blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." A blockchain is usually maintained via a peer-to-peer network that follows a common protocol for verifying new blocks in order to function as a distributed ledger. Once recorded, the data in a block cannot be changed backward without changing all blocks that come after it, which calls for the majority of the network to operate together. Digital money, like Bitcoin, is the most straightforward and widely used blockchain application. Bitcoins, in contrast to conventional money, are totally virtual. Coins, either real or digital, do not exist in and of themselves. In transactions when value is transferred from sender to receiver, the coins are inferred. Bitcoin users own keys that enable them to authenticate transactions inside the network, releasing the value so they may spend it or give it to another person. Usually, each user's computer has a digital wallet where such keys are kept. The sole need to spend bitcoins is to have the key that unlocks the transaction, giving each user complete power. These days, an increasing number of businesses and entrepreneurs are utilizing blockchain in finance records, medical records, and other records management activities, like identity management, transaction processing, documenting provenance, or food traceability, due to its decentralization, trustlessness, collective maintenance, and dependability.

2.4 BLOCKCHAIN-BASED IDENTITY MANAGEMENT WITH MOBILE DEVICE

In this study, Zhimin Gao, et al. have suggested When it comes to transactions requiring a centralized, transparent, robust, and consensus-based record keeping system, blockchain is a powerful and distributed platform. It has been used in situations including supply chains, smart cities, the sharing and keeping of medical data, and more. Numerous efforts have been made to enhance these systems' security and performance. But when a person engages in comparable physical world activities, there is no identity binding mechanism in place. That is to say, if a person engages in an activity, their identity in the actual world ought to be accurately mirrored in the block chain system. We suggest Block ID, a cutting-edge system for managing people's identities that makes use of trusted computing and biometric verification, to close this gap. In order to show that it is feasible in real life, we also create a prototype. The database that powers Bitcoin is often referred to as block chain. A collection of independent users maintains the block chain, which is a decentralized ledger. By using a consensus process, users may add new blocks to the block chain by attaching the evidence to the freshly created block and solving a computationally demanding challenge. It is simple for everyone who gets the new block to confirm the evidence and ascertain whether or not the new block is legitimate. An attacker cannot alter any record as long as the majority of users remain truthful since they must own over 50% of the system's processing power. Block chain is an effective technique for managing data online. The actual world and the cyber world must be reliably mapped in order for such a system to reach its full potential. RFID technology and other digital tagging systems may be used for this, using cargos as an example. However, supply chain participants do the mapping manually or with the use of pricey, specialized equipment [11]. As a result, a more affordable method of connecting individuals to the digital world that works with block chain technology is required.

2.5 BLOCKCHAIN-BASED IDENTITY MANAGEMENT SYSTEMS: A REVIEW

In this research, Yang Liua et al. have proposed Identity management solutions are extensively used in real-world applications, and they are often designed to make managing digital identities and tasks like authentication easier. Attempts have been made in recent years to implement identity management systems based on blockchain technology, which provide users the ability to take charge of their own identities (also known as self-sovereign identities). In this work, we provide a thorough analysis of the literature on identity management using block chain technology, including articles and patents issued between May 2017 and January 2020. We highlight prospective research gaps and opportunities based on the literature analysis, which should assist shape the future research agenda. Keywords: self-sovereignty, block chain, identity management system, and block

chain-based identity management. Our digitalized, networked world is becoming more and more dependent on digital identities. For instance, the majority of us have many digital personas connected to our personal, professional, and work-related activities. In order to manage and safeguard our identity information and to deliver pertinent services, identity information management also known as identity management, identity management and access control, etc. is becoming more important. This is partially due to this. Attempts have also been made to include blockchain into the design of the next generation of identity management systems, building on the success of blockchain technology. Numerous dispersed nodes make up a typical blockchain-based identity management system [4]. These nodes may be used to provide compute power, dependable access, and distributed storage. Since the user in such a system functions as a node in the network, sensitive user data may now be stored on user devices or nodes rather than servers as in traditional identity management systems (in the new blockchain-based paradigm). The capacity for people to take back control of their identities makes self-sovereign identification (SSI) easier. As such, this reduces a number of hazards associated with traditional identity management systems. It is not unexpected that there are still a lot of difficulties since block chain-based identity management solutions are a relatively new trend. How, for instance, may users persuade establishments to voluntarily adopt characteristics of unreliable pseudonymous people? If a transaction is later shown to be fraudulent or illegal and the organizations failed to take reasonable steps to confirm the identity of the people engaged in the transaction, there may also be financial and legal repercussions

3. EXISTING SYSTEM

Identity theft is the unlawful taking of another person's private information with the intention of abusing it. To prevent fraud resulting from identity theft, both people and organizations should use prudence when it comes to identity protection. Attackers may easily get this data via user profiles. Attackers exploit this data to gather more information without giving rise to concerns about fraud, identity theft, or a final assault. Our block chain-powered Personal identification Security System helps to safely store personal identification information so that you don't have to worry about it becoming lost or hacked. The administrator of this system has access to every user and may confirm their identities. Every document that a user uploads to the system is accessible to the administrator. All of the user's activity logs are visible to them. The administrator may check the status and determine if any fabrication is occurring. The user's concerns are seen by the admin.

4. PROPOSED SYSTEM

The solution under consideration is a complete personal identity security system that utilizes block chain technology and the SHA-256 algorithm to improve data integrity. It includes an easy-to-use Login module for safe authentication, a User Signup module for establishing accounts with necessary personal information, and a Home module that shows important block chain data. The Keys module generates public and private keys, which are necessary for safe transactions and provide strong cryptographic security. By creating a digital identity for users, the Identify module improves verifiability and privacy. Finally, private keys for financial transactions are securely managed by the Bank Account module. Through the integration of various components, the system offers a transparent and decentralized structure that protects individual identities and guarantees data integrity within an unchangeable blockchain framework. By reducing the dangers connected with centralized identity management, this strategy provides banks and users with a dependable and safe option in the constantly changing digital environment.

4.1 LOGIN

By requiring a username and password, the login module offers banks and users a safe authentication method. In order to customize access rights, it differentiates between normal users and banks based on responsibilities.

4.2 USER SIGN-UP

Through the collection of necessary data, including first and last name, email address, cell phone number, username, and password, user registration makes it easier to create new accounts. The basis for user involvement in the block chain-based identity security system is laid forth in this module.

4.3 HOME

The Home module, which shows important details for every block, contains all of the block chain system's essential features. This contains the hash of

the previous block, the hash of the current block, the block number, the timestamp, the contents, and the nonce (a cryptographic integer). By gaining access to the block chain's structure, users may verify the accuracy of the data contained within.

4.4 KEYS

In order to ensure cryptographic security, public and private keys must be generated via the Keys module. These keys are essential for maintaining the secrecy and authenticity of system communications and transactions.

4.5 IDENTIFY

The purpose of the Identify module is to provide users in the block Chain system a digital identity. In order to protect user privacy, facilitate safe transactions, and create a distinct and authenticated presence on the block chain, this digital identity is essential.

4.6 BANK ACCOUNT

A user's private key is stored and managed in the Bank Account module. This is an essential component of safeguarding their bank account access on the block chain. By guaranteeing the integrity and secrecy of financial transactions, this module strengthens the user's digital identity's overall security.

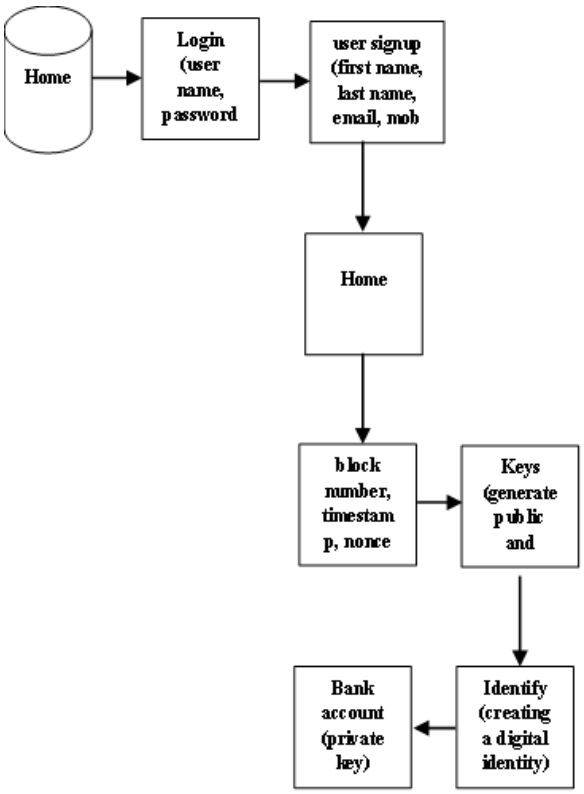

Figure 1SYSTEM ARCHITECTURE

ALGORITHM DETAILS

A text or data file may be signed using the SHA 256 technique, often known as a digest. A text may be signed with a nearly unique 256-bit (32-byte) signature using SHA-256. A hash is a cryptographic "one-way" characteristic that has a set size for all source text sizes; unlike encryption, it cannot be decoded back to the original text. Because of this, it's perfect for comparing "hashed" copies of texts instead of decrypting them to get the original version.

Basic Initialization will be done for 8 items

Step 1: Information is a array 8 things in length where every thing is 32 bits.

Step 2: out is a array 8 things in length where every thing is 32 bit.

Step: 3 Compute all the capacity boxes and store those qualities. Allude to them by work name

Step: 4 Store input, right moved by 32 bits, into out. Now, in the out exhibit, E is an inappropriate worth and A is unfilled

Step: 5 Store the capacity boxes. Presently we have to compute out E and out A. note: Supplant the modulo orders with a bitwise AND 2^(32-1)

Step : 6 Store (Input I + CH + ((XT+YT) AND 2^31)) AND 2^31 As Mod1

Step : 7 Store (Sum1 + Mod1) AND 2^31 as Mod2

Step : 8 Store (b + Mod2) AND 2^31 into out E Presently out E is right and all we need is out A

Step : 9 Store (NA + Mod2) AND 2^31 as Mod3

Step : 10 Store (Sum0 + Mod3) AND 2^31 into output

5. RESULT ANALYSIS

The suggested approach shows a significant increase, obtaining an accuracy rate of 88%, compared to the present algorithm's 75% accuracy rate. This improvement points to a significant improvement in the suggested algorithm's ability to handle and analyze data effectively or carry out its intended function. Numerous variables, including optimization approaches, algorithmic modification, or the incorporation of more reliable data preparation methods, may contribute to the suggested algorithm's increased accuracy. This

improvement in accuracy highlights the suggested algorithm's ability to provide more dependable outcomes and favorably impact its targeted application area.

algorithm	accuracy
Existing	75
Proposed	88

Table 1. Comparison table

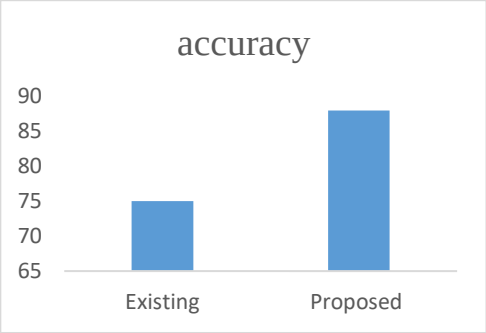

Figure 2. Comparison graph

6. CONCLUSION

To sum up, the suggested blockchain-based SHA-256 encryption personal identity security system offers a strong and creative response to the problems associated with protecting digital identities. The system assures data integrity, user privacy, and secure financial transactions in addition to establishing a decentralized and transparent framework via the integration of modules including Login, User Signup, Home, Keys, Identify, and Bank Account. User-friendly input and output interfaces are given priority in the design, which improves usability and accessibility. The system's objective is to mitigate the dangers associated with centralized identity management and promote confidence in an increasingly digital environment by offering a dependable and robust platform for users and banks, via methodical testing and deployment. Because of the thorough methodology used throughout the development and implementation phases, the system is positioned as a viable and efficient means of handling the ever-evolving complexity of personal identity security.

7. FUTURE WORK

The personal identification security system based on blockchain may be improved in the future by being innovative and adjusting to new technology. Integrating smart contracts and sophisticated consensus techniques might improve the security and usefulness of the system even further. Examining the integration of verified credentials and decentralized identifiers (DIDs) might improve the interoperability and scalability of digital identities. In addition, the system may benefit from investigating biometric authentication techniques to offer one more degree of user verification.

8. REFERENCE

[1] R. Kumar, A. Malik, and V. Ranga, "Identification Verification System via Blockchain Technology," Nov. 2022, vol. 256, art. no. 109762, Knowledge-Based Systems.
[2] BPDIMS: A Blockchain-based Personal Data and Identity Management System, W. Wang, S. Jian, Y. Tan, Q. Wu, and C. Huang, Comput. Secur., vol. 112, Jan. 2022, Art. no. 102537.
[3] "Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging," by J. Oughton, W. Lehr, K. Katsaros, I. Selinis, D. Bubley, and J. Kusuma June 2021, Telecom Policy, vol. 45, no. 5, Art. no. 102127 In February 2021, B. A. Tama and S. Lim published "Blockchain-based Identity Management with Mobile Device" in Computer Science and Engineering Review, vol. 39, art. no. 100357.
[5] "Blockchain-Based Identity Management Systems: A Review," by S. Lei, C. Xia, Z. Li, X. Li, and T. Wang IEEE Trans. Netw. Sci. Eng., Oct. 20, 2021, vol. 8, no. 4, pp. 3257–3274
[6] "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," by Y. Cheng, Y. Xu, H. Zhong, and Y. Liu IEEE Internet Things Journal, Jan. 2021, vol. 8, no. 1, pp. 144–155.
[7] "DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network," by X. Li, M. Zhu, L. T. Yang, M. Xu, Z. Ma, C. Zhong, H. Li, and Y. Xiang IEEE Transactions on Dependable Secure Computing, vol. 18, no. 4, July/Aug. 2021, pp. 1591–1604
[8] A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain, Y. Zhou, G. Cheng, S. Jiang, and M. Dai, Comput. Netw., vol. 174, Jun. 2020, Art. no. 107247.
[9] "Blockchain for Identity Management," G. Kumar, K. Thakur, and M. R. Ayyagari, J.

Supercomput., vol. 76, no. 11, pp. 8938–8971, Nov. 2020
[10] "A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems," by B. A. Tama, L. Nkenyereye, S. M. R. Islam, and K. Kwak IEEE Access, volume 8, 2020, pages 24120–24134.