BLOCKCHAIN-BASED DATA PROTECTION AND SECURING INFORMATION WITH SHA256 ALGORITHM

VIJAYA LAKSHMI D M [1], KIRAN BABU N [2] ,MOHANKUMAR S [3],

NAVEEN KUMAR S [4], PUNITH RAJ R [5]

[1]Assistant Professor, [2][3][4][5]UG Scholars,

Department of Computer Science Engineering,

Adhiyamaan College of Engineering, Hosur, India.

ABSTRACT- The security of data is of utmost importance in today's digital age, and with the increasing amount of data being generated, it has become imperative to ensure that sensitive data is protected from unauthorized access or tampering. Blockchain technology provides a secure and decentralized way to store and manage data, making it an ideal solution for securing sensitive data. This paper proposes a secure data processing system that uses blockchain technology and the SHA256 algorithm. The proposed system consists of three main components: a data processing module, a blockchain module, and a user interface module. The data processing module is responsible for processing and encrypting the data using the SHA256 algorithm. The encrypted data is then stored on the blockchain, which provides a decentralized and tamper-proof way to store the data. The user interface module allows users to access and interact with the system, enabling them to securely share and retrieve data. The SHA256 algorithm is used to encrypt the data because it is a secure and widely used cryptographic hash function that produces a fixed-length output that is unique to the input. This ensures that the data cannot be tampered with, as any changes to the data will result in a different hash output. The blockchain module provides a tamper-proof way to store and manage the encrypted data. Blockchain technology uses a distributed ledger that is replicated across multiple nodes, ensuring that the data is decentralized and cannot be altered without the consensus of the network. This provides a high level of security and transparency, as all changes to the data are recorded on the blockchain and can be audited at any time. The user interface module allows users to securely access and interact with the system. Users can upload and retrieve encrypted data from the blockchain using a private key that is generated for each user. This ensures that only authorized users can access the data, and any unauthorized access attempts will be denied.

INTRODUCTION

In today's digital world, data security has become a critical concern for individuals and organizations alike. With the increasing amount of data being generated and shared, the need for secure data processing systems has become more important than ever. In response, blockchain technology has emerged as a promising solution to address the challenges of data security.Blockchain technology is a decentralized and distributed ledger that is highly secure and tamper-proof. It provides a secure way to store and manage data, making it an ideal solution for organizations that require a high level of security and transparency for their sensitive data. The SHA256 algorithm is a widely used cryptographic hash function that produces a fixed-length output that is unique to the input. It is highly secure and widely used in various cryptographic applications. Blockchain technology is a decentralized and distributed ledger that is highly secure and tamper-proof. It provides a secure way to store and manage data, making it an ideal solution for organizations that require a high level of security and transparency for their sensitive data. The SHA256 algorithm is a widely used cryptographic hash function that produces a fixed-length output that is unique to the input. It is highly secure and widely used in various cryptographic applications. The proposed system combines the use of blockchain technology and the SHA256 algorithm to provide a secure data processing solution. The system consists of three main components: a data processing module, a blockchain module, and a user interface module. The data processing module is responsible for processing and encrypting the data using the SHA256 algorithm. The encrypted data is then stored on the blockchain, which provides a decentralized and tamper-proof way to store the data. The user interface module allows users to access and interact with the system, enabling them to securely share and retrieve data. The proposed system provides several benefits, including increased security, transparency, and efficiency. By using blockchain technology and the SHA256 algorithm, the system ensures that data is secure and cannot be tampered with, while the decentralized nature of the blockchain ensures that the data is available to authorized users at all times. The user interface module also enables users to securely access and interact with the system, making it easy to use and highly efficient. Overall, the proposed system provides a highly secure and efficient solution for data processing that is ideal for organizations that require a high level of security and transparency for their sensitive data.

OBJECTIVE

The objective of the proposed system for secure data processing using blockchain and SHA256 algorithm is to provide a highly secure, decentralized, and tamper-proof solution for data processing. The system aims to address the challenges of data security in today's digital world by using blockchain technology and the SHA256 algorithm to ensure that data is encrypted and cannot be tampered with. The system also aims to provide a transparent and efficient way to store and manage data, making it easy for authorized users to access and interact with the system. Ultimately, the objective of the proposed system is to provide a reliable and secure solution for organizations that require a high level of security and transparency for their sensitive data.

LITERATURE REVIEW

1.VABKS: Verifiable attribute-based keyword search over outsourced encrypted data Q. Zheng, S. Xu, and G. Atenas,

It is very normal these days for information proprietors tore-appropriate their information to the cloud. Since the cloud isn't completely trusted, the reevaluated information ought to be encoded, which anyway brings a scope of issues, for example, How might the approved information clients search over an information proprietor's reevaluated encoded information? How might an information proprietor award search capacities to information clients? How might information clients be guaranteed that the cloud steadfastly executed the hunt procedure for their sake? Towards at last resolving these issues, in this paper we propose an original cryptographic arrangement, called undeniable trait based

watchword search (VABKS). This arrangement permits an information client, whose qualifications fulfill an information proprietor's entrance control strategy, to (I)search over the information proprietor's rethought encoded information, (ii)

re-appropriate the monotonous hunt activities to the cloud, and (iii)check whether the cloud has reliably executed the client's the tasks. We characterize VABKS's security properties and present substantial developments that are demonstrated to fulfill them.

Execution assessment shows that the proposed plans

commonsense and deployable.

2. Protecting your right: Attribute-based keyword search with fine-grained owner-enforcedsearch authorization in the cloud,”

W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li,

Search over encoded information is a basically significant empowering method in distributed computing, where encryption-before-re-appropriating is a major answer for safeguarding client information protection in the untrusted cloud server climate. Many secure hunt plans have been zeroing in on the single-donor situation, where the rethought dataset or the protected accessible record of the dataset are encoded and overseen by a solitary proprietor, regularly founded on symmetric cryptography. In this paper, we center around an alternate yet really testing situation where the rethought dataset can be contributed from numerous proprietors and are accessible by different clients, for example multi-client multi-supporter case. Propelled by characteristic based encryption (ABE), we present the main quality based catchphrase search conspire with effective client disavowal (ABKS-UR) that empowers adaptable fine-grained (for example document level) search approval. Our plan permits numerous proprietors to autonomously encode and re-appropriate their information to the cloud server. Clients can create their own hunt capacities without depending on a consistently online confided in power. Fine-grained search approval is additionally carried out by the proprietor implemented admittance strategy on the list of each document. Further, by consolidating intermediary re-encryption and languid re-encryption strategies, we can designate weighty framework update responsibility during client disavowal to the creative semi-confided in cloud server. We formalize the security definition and demonstrate the proposed ABKS-UR plot specifically secure against picked catchphrase assault. At long last, execution assessment shows the effectiveness of our plan.

3.**An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud, Mamta and B. B. Gupta**

Attribute-based accessible encryption (ABSE) is the mix of attribute-based encryption (ABE) and accessible encryption with the innate advantages of fine-grained access control and expressive looking through capacities in multiuser setting. In this paper, we have utilized the key-policy (KP) plan system of ABE and named the plan KP-ABSE. The proposed KP-ABSE plot proficiently upholds client renouncement where the computationally concentrated undertakings are designated to the cloud server. Moreover, the proposed conspire produces constant-size client secret keys and hidden entryways and has steady number of matching tasks, which in different plans regularly changes with the quantity of properties related with them. Subsequently, the proposed plot diminishes computational and stockpiling expenses and supports quick looking. At last, the proposed plan can be demonstrated secure under a choice straight supposition in a specific security model.

4. **Secure fine-grained keyword search with efficient user revocation and traitor tracing in the cloud Mamta and B. B. Gupta,**

Fine-grained looking is a significant component in multi-client cloud climate and a blend of characteristic based encryption (ABE) and accessible encryption (SE) is utilized to work with it. This mix gives a useful asset where numerous information proprietors can impart their information to various information clients in a free and differential way. In this article, the writers have utilized key-strategy plan structure of trait-based encryption to build the multi-watchword search plot where access privileges doled out to an information client are related with his/her mystery key. This prompts what is going on where an information client can manhandle his mystery key to circulate it illicitly to the unapproved clients to perform search over the common information which isn't expected for him/her. Consequently, to track such sort of key victimizers the creators have inserted an additional usefulness of following the tricksters. For this reason, every client is doled out a novel character as parallel string where each piece addresses a property connected with his personality. Notwithstanding the ordinary credits, the entrance construction of a client likewise has character related ascribes which are stowed away from the client alongside a few typical properties. Thus, the proposed conspire upholds incomplete obscurity. Further, in case of client renouncement the proposed conspire productively handles the framework update process by designating the computationally serious assignments to the cloud server. At last, the proposed plot is demonstrated secure under Decisional Bilinear Diffie-Hellman (DBDH) suspicion and choice direct presumption in the specific security model.

5.Attribute-based multikeyword search over encrypted personal healthrecords in multi-owner setting

Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang

As various patients' information is constantly put away in the cloud server all the while, it is a test to ensure the secrecy of PHR information and permit information clients to look through encoded information in an effective and protection saving way. To this end, we plan a solid cryptographic crude called as characteristic based multi-watchword search over encoded individual wellbeing records in multi-proprietor setting to help both fine-grained admittance control and multi-catchphrase search by means of Ciphertext-Strategy Property Based Encryption. Formal security examination demonstrates our plan is specifically secure against picked watchword assault. As a further commitment, we lead exact examinations over genuine world dataset to show its plausibility and reasonableness in an expansive scope of genuine situations without causing extra computational weight**.**

Existing System

The current frameworks are poor in handling huge volumes of multi-organized medical care information with less security utilizing AES Algorithm and not giving precise wellbeing proposal information.

Disadvantage of Existing System

Problem transformation method first transforms one multilabel dataset into multiple single-label datasets, and then exploits existing single-label learning algorithm to process each single-label dataset.

PROPOSED SYSTEM:

Data Encryption: The data that needs to be secured is first encrypted using the SHA256 algorithm, which generates a unique 256-bit hash value for the data. Data Storage: The encrypted data is then stored in a block, which is linked to the previous block in a blockchain. This creates an immutable ledger of all the data that has been processed, making it tamper-proof. Consensus Mechanism: In order to maintain the integrity of the blockchain, a consensus mechanism is used. This mechanism ensures that all nodes in the network agree on the state of the blockchain, and that no single entity can alter the data stored in the blockchain.

Advantages

Immutability data stored in a blockchain using SHA256 algorithm is tamper-proof and immutable, which means that once data is added to the blockchain, it cannot be altered or deleted. Security the use of cryptography in the form of public and private keys ensures that only authorized parties can access and modify the data stored in the blockchain. Decentralization the blockchain network is decentralized, which means that there is no single point of failure, and the data stored in the blockchain is distributed across multiple nodes, making it highly resilient to attacks Transparency all transactions that are processed on the blockchain are transparent and can be audited, which makes it ideal for applications where transparency is important such as supply chain management.

MODULES

- Register and Login
- Cipher Text Encryption
- Cipher Text Decryption
- Block Chain Crypto System Algorithm

Register and Login

- Register as client by giving first name, last name, client name and secret key, and so forth...
- Login Utilizing Client Name and Password.

Cipher Text Encryption

- Figure message is the message acquired in the wake of applying cryptography on plain message.
- The most common way of changing plain text over completely to encode text is called encryption. It is additionally called as encoding**.**

Cipher Text Decryption

- Symmetric encryption is a method for encoding or conceal the items in material where the source and beneficiary both utilize a similar mystery key. Note that symmetric encryption isn't adequate for most applications since it just gives mystery yet not legitimacy.
- That implies an assailant can't see the message yet an aggressor can make sham messages and power the application to decode them

Block Chain Crypto System Algorithm

- Utilizing Block chain Calculation information of every patient will be Encoded In light of Cryptographic procedure.
- Encoded information from data set is displayed to proper specialist and patient with decoded design

HARDWARE REQUIREMENTS

- System: I3 Processer
- Hard Disk: 500 GB.
- Monitor: 15 VGA Color.
- Ram: 4 Gb

SOFTWARE REQUIREMNET

- Windows 10
- Visual Studio 2022
- MSSQL SERVER 2019

Conclusion

In this paper, secure data processing using blockchain and SHA256 algorithm offers a highly secure and efficient way of processing and storing data. The use of cryptography, decentralization, transparency, and consensus mechanisms ensures that data stored in a blockchain is tamper-proof, secure, and can only be accessed by authorized parties. Additionally, the distributed nature of the blockchain network ensures that the data is highly resilient to attacks and has no single point of failure. This technology has a wide range of potential applications, including supply chain management, financial transactions, and identity management, among others. Overall, secure data processing using blockchain and SHA256 algorithm provides a robust and reliable solution for secure data processing and storage.

References

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org.

https://bitcoin.org/bitcoin.pdf

2. Swan, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media, Inc.

3. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: beyond bitcoin. Applied Innovation, 2(6-10), 71-81.

4. Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc.

5. Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9).

6. Pilkington, M. (2015). Blockchain technology: principles and applications. Research Handbook on Digital Transformations, 225-253.

7. Zhang, Y., Wen, Q., & Hu, Y. (2018). A blockchain-based approach to enhancing data security and privacy in cross-domain healthcare information systems. Journal of medical systems, 42(8), 141.

8. Kshetri, N. (2018). Blockchain’s roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

9. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., & Bass, L. (2017). A taxonomy of blockchain-based systems for architecture design. Proceedings of the 2017 International Conference on Software Architecture, 243-252.

10. Sun, X., & Zhang, Z. (2016). A new method for data security and privacy protection in cloud computing based on blockchain technology. Journal of Information Security and Applications, 31, 1-

11. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems, 82, 1-14.

12. Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Chen, X. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 13(2), 115-131.

13. Dinh, T. T. A., Wang, J., Chen, G., Liu, R., & Ooi, B. C. (2018). A comprehensive survey of blockchain: From theory to applications. ACM Computing Surveys, 51(4), 1-36.

14. Kumar, V., & Tripathi, M. (2019). Blockchain based secure data processing: A review. Journal of King Saud University-Computer and Information Sciences, 31(4), 508-520.

15. Zheng, Z., Xie, S., & Yang, Y. (2019). Blockchain challenges and opportunities: A survey of the current state-of-the-art. International Journal of Information Management, 49, 84-96.

16. Yin, C., Yao, L., & Wu, Y. (2020). Blockchain-based secure and privacy-preserving data sharing scheme for healthcare systems. IEEE Transactions on Industrial Informatics, 16(1), 98-107.

17. Hao, F., & Zhang, L. (2019). A secure data sharing scheme based on blockchain technology. Security and Communication Networks, 2019, 1-12.