IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Implementing A Technique To Enhance The Logistic System Privacy And Traceability Using Blockchain

[1]Sushant Buche, [2]Prathamesh Misal, [3]Sahil Halmare, [4]Gaurav Divtelwar

[1-3]Projecties, [4]Assistant Professor
Department Of Computer Technology
Kavikulguru Institute of Technology and Science, Ramtek, India

Abstract: To ensure the security of logistics information and to query information quickly and efficiently using searchable encryption algorithms and blockchain characteristics, a searchable and encrypted logistics information blockchain data query algorithm is proposed. The logistical data is initially divided into numerous data files before being deposited in the cloud server.The data is encrypted and stored using an asymmetric searchable encryption mechanism. The keyword index value of each data file is extracted and submitted to the blockchain. This solution can be applied at any time. Updates and inquiries on data. Next, assess the article's plan's correctness, completeness, and security, which proves its feasibility.

Keywords **– Blockchain, searchable encryption, asymmetric encryption, logistics information, data query.**

I. INTRODUCTION

With the fast rise of e-commerce in recent years, the logistics sector's business volume has seen an exponential growth pattern. Logistics management is becoming increasingly informative because of the Internet industry's quick changes, and its techniques, means, and strategies are evolving towards intelligence. Yet, there are a lot of issues that still need to be resolved behind this trend. Logistics linkages cover a wide geographic region and take a long time to complete, making oversight challenging and the elimination of counterfeiting challenging. When Satoshi Nakamoto created Bitcoin in 2008, it quickly gained popularity all around the world. Because of its decentralization, tamper resistance, and traceability, Bitcoin's blockchain technology has garnered considerable interest from academics both domestically and internationally. Blockchain technology can address the issue of excessive influence in traditional logistics companies' "central" organization. Real-time viewing and information transmission are assured by the creation of a transparent, uniform information platform by several parties, allowing for the ability to trace back any information in the chain from manufacturing to transportation. In the entire information transmission process, the logistics blockchain is formed through data encryption and consensus verification, thereby ensuring the authenticity and transparency of logistics service transaction information and ensuring that the information will not be tampered with and can be queried and traced to the source. Blockchain can accommodate all users in the logistics service process. By utilizing its technological components, such as distributed storage, encryption algorithms, and timestamps, blockchain technology successfully addresses the drawbacks of conventional tracing systems. According to the traits of their constituents, the many blockchain varieties may be categorized into public chains, consortium chains, and private chains. The term "consortium chain" describes a blockchain network that is solely accessible to certain group members and a small number of third parties.

II. LITERATURE SURVEY

S. F. Niu, W. K. Liu, and L. X. Cheng, ‘‘Electronic medical record data sharing scheme based on searchable encryption via consortium blockchain,’’ The immutability of the data recorded in the blockchain increases its security. In this paper, we propose a blockchain-based system for sharing data from electronic medical records, which enables data users from third parties to exchange patient information without invading their privacy. We start by offering a system model for the plan. A private blockchain and a consortium blockchain are used to build the system. The patient's diagnostic record is kept on a private blockchain (DR). DRs' keywords are stored in safe indexes on the consortium blockchain. Keywords and diagnostic reports are stored as encrypted ciphertext data.Second, we implement a secure keyword search on the consortium blockchain using public encryption with keyword search (PEKS) technology. Proxy re-encryption (PRE) technology is used at the decryption stage to give third-party data users secure access to patient data. Lastly, we conduct numerical simulation tests to assess the scheme's performance.[1].

L. Zhang, Z. Y. Zheng, and Y. Yuan, ‘‘A controllable sharing model for electronic health records based on blockchain, ’The development of electronic medical records has greatly facilitated the analysis and storage of medical data. Even though electronic medical records contain a lot of information about a person's privacy, sharing medical data between different medical institutions is still quite challenging. Blockchain technology, which underpins Bitcoin, has the properties of decentralization, security, reliability, community upkeep, and cannot be altered, making it appropriate for data sharing and protection. The Inter Planetary File System (IPFS) and data masking technologies are discussed in this study to create a secure and effective blockchain-based electronic medical

record sharing paradigm. The technique can save resources in blockchain while simultaneously ensuring the confidentiality of medical data.[2].

L. G. CH and Q. LI, ‘‘Blockchain data privacy protection mechanism based on searchable encryption, ’The security of our society depends on data privacy, and making it possible for authorized users to easily query this data is becoming more difficult. With its significant attributes of public, distributed, decentration, and chronological features, blockchain has recently attracted a lot of interest. Yet, since all nodes can see the transaction information on the blockchain, updating the transaction information is much more transparent. Also, the transaction party may suffer significant damages if transaction information is disclosed. In response to these issues, this paper proposes a blockchain data privacy protection control scheme based on searchable attribute encryption, which addresses the issue of privacy exposure in conventional blockchain transactions. It does this by fusing hierarchical attribute encryption with linear secret sharing. The verification nodes handle user access control, avoiding the security concerns associated with transmitting private keys and access hierarchies to the blockchain network. The collusion issue may be resolved by coupling the private key component with the arbitrary user node identification in the blockchain. Also, using searchable encryption, authorized individuals may instantly examine and monitor transaction information. The enhanced algorithm guarantees the confidentiality of keywords. Lastly, based on the DBDH premise, the random prediction proves the scheme's security.[3].

H. Qin, Z. Li, P. Hu, Y. Zhang, and Y. Dai, ‘‘Research on point-to-point encryption method of power system communication data based on block chain technology,’’ A point-to-point encryption technique of power system communication data based on block chain technology has been researched and developed in response to the lack of stability of conventional communication data encryption methods. The design technique uses the decentralization and consensus mechanism of block chain technology to construct the public key distribution scheme in accordance with the principle of asymmetric key encryption. The sender and receiver of communication data produce the transfer key when the public key distribution is finished, then pair the key with the public key to achieve the pairing between data points. The communication data content is subjected to Xor and modular exponentiation, and prime numbers are employed to fill the content data block. The receiver completes the design of the encryption method of transmission data point to ground by decrypting the data in accordance with the encryption identifier of the data content. It has been demonstrated via comparison to the conventional encryption technique that the more encrypted data there is, the more secure the communication data can be, and the performance of stability is superior to the conventional encryption method.[4].

J. Sun, L. Ren, S. Wang, and X. Yao, ‘‘Multi-keyword searchable and data verifiable attribute-based encryption scheme for cloud storage, ’It is a fundamental necessity in a data sharing system for a user to be able to execute keyword retrieval for encrypted documents kept in the cloud. Even though data security and retrieval capabilities may be provided by typical searchable encryption technology, there are certain major difficulties that must also be considered. First off, most attribute-based searchable encryption systems in use today only enable single-keyword searches, which can provide a large number of useless search results and waste bandwidth and computing resources. Second, the user constantly wants to find information pertaining to certain terms, yet his characteristics may frequently change. Finally, because the cloud server isn't always trustworthy, occasionally some incorrect search results are returned. By merging the ciphertext policy attribute-based encryption (CP-ABE) and auditing concepts, a workable multi-keyword searchable encryption system is provided for data integrity verification and attribute revocation. The plan, which supports multiple keywords, prevents the cloud server from returning many irrelevant documents by focusing the search. On the other hand, it can successfully implement attribute revocation by entrusting ciphertext updates to the powerful cloud server, preventing access from unauthorized users. Moreover, third-party audits employ verification algorithms to lessen the amount of work required from end users while ensuring the accuracy of search results. Most importantly, under the generic group model, the technique demonstrated resistance to selective plaintext attacks and selective keyword assaults. The system is more expressive, efficient, and practical in the applications, as shown by the substantial experimental findings.[5].

S. Tahir, S. Ruj, Y. Rahulamathavan, M. Rajarajan, and C. Glackin, ‘‘A new secure and lightweight searchable encryption scheme over encrypted cloud data,’ A new cryptographic method called searchable encryption makes it possible to browse through encrypted data stored in the cloud. An innovative searchable encryption method for client-server architecture has been introduced in this work. The method takes advantage of the modular inverse's characteristics to create a probabilistic trapdoor that makes it easier to search through the secure inverted index table. We suggest indistinguishability, which is attained by utilizing a probabilistic trapdoor's feature. We create and put into practice a proof-of-concept prototype, then use an actual dataset of files to test our system. We compare the effectiveness of our plan to the assertion that it is lightweight. Our plan guarantees a greater level of security than other current schemes, according to the security study.[6].

III. Existing Method

For blockchain applications to be successful in the e-finance, e-commerce, and logistics industries, relational and analytical queries are essential. Because of this, the current blockchain system's query capabilities is severely limited, making it difficult to meet the requirements of second- and current-generation transaction applications.

- If there are too many users on the network, the blockchain can slow.
- Information cannot be changed since it is immutable.
- Blockchains are useless due to the way they work.
- Scaling is challenging due to the consensus process.

IV. Proposed System

The recommended methodology uses symmetric encryption to encrypt private data before transmitting it to a cloud storage provider. The rapid attribute-based encryption method is then used to encrypt the symmetric key k. The blockchain is then updated with the newly produced ciphertext CT. It is composed of the key ciphertext CT1 and the access policy CT2, respectively. The blockchain's decentralization and tamper-proof features safeguard the integrity of the key ciphertext and access policy. This technique considerably reduces the computation needed for encryption and decryption, enhancing the efficacy of the recommended strategy.

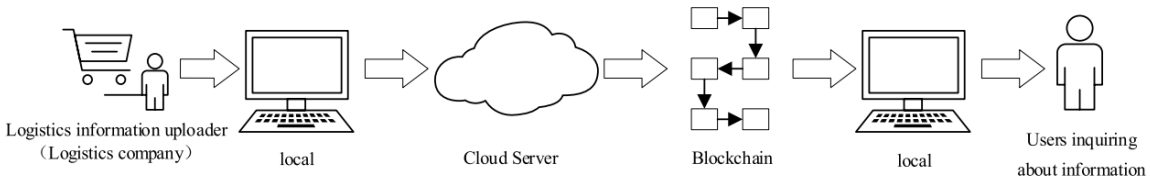

Figure 1: Searchable encryption application process

- Requirement gathering and analysis - During this stage, all potential system needs are gathered and outlined in a requirement specification document.
- System Design - In this step, the required specifications from the previous phase are examined, and a system design is created. This system design aids in determining the overall system architecture as well as the hardware and system requirements.
- Implementation - The system is initially created as a collection of short programs known as units, which are then combined in the next phase, using input from the system design. Unit testing is the process of developing and evaluating each unit for functionality.
- Integration and Testing - Following the testing of each unit created during the implementation phase, the entire system is integrated. The entire system is tested for errors and failures after integration.
- System deployment - After functional and non-functional testing, the product is either provided to customers or deployed in their environments.
- Maintenance - The client environment occasionally experiences problems. Patches are published to address certain problems. Moreover, various improved versions of the product have been launched. To bring about these changes in the surroundings of the consumer, maintenance is performed.

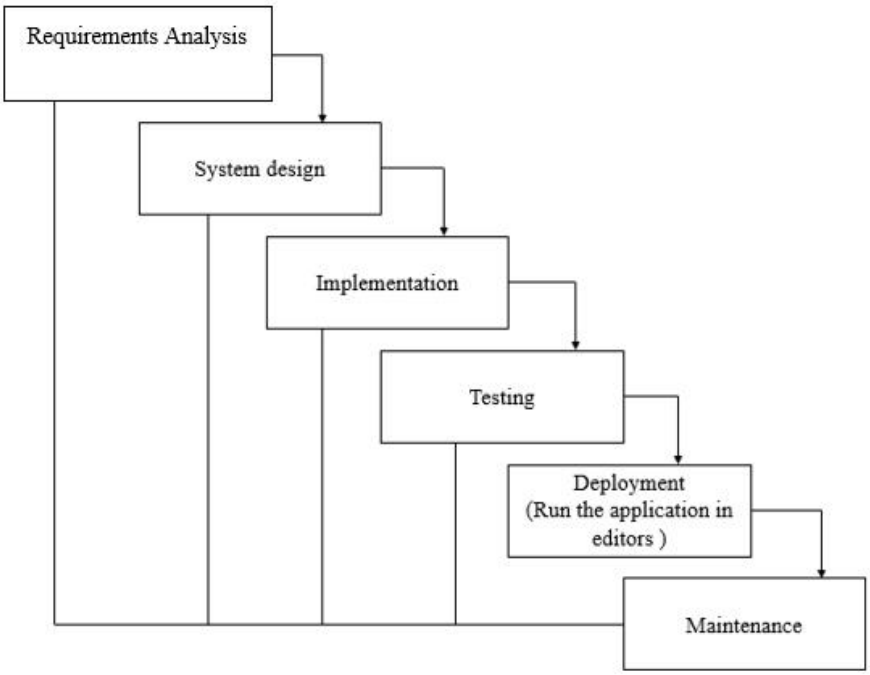

Figure 2: Waterfall model

4.1 System Architecture

The workflow of the project is shown by the figure below, in which the uploader uploads the details of the items that are available to him/her. The published Data files are subsequently delivered with the information to the server. Nonetheless, it is simple to alter the data files that are uploaded to the cloud server. As a result, the data files are transferred to the blockchain, where they are divided into individual blocks and kept in chains. Here, a distinct hash function is assigned to each block, protecting the data files from unwanted access. Only those with access to the website can view the data that is stored on the cloud server.

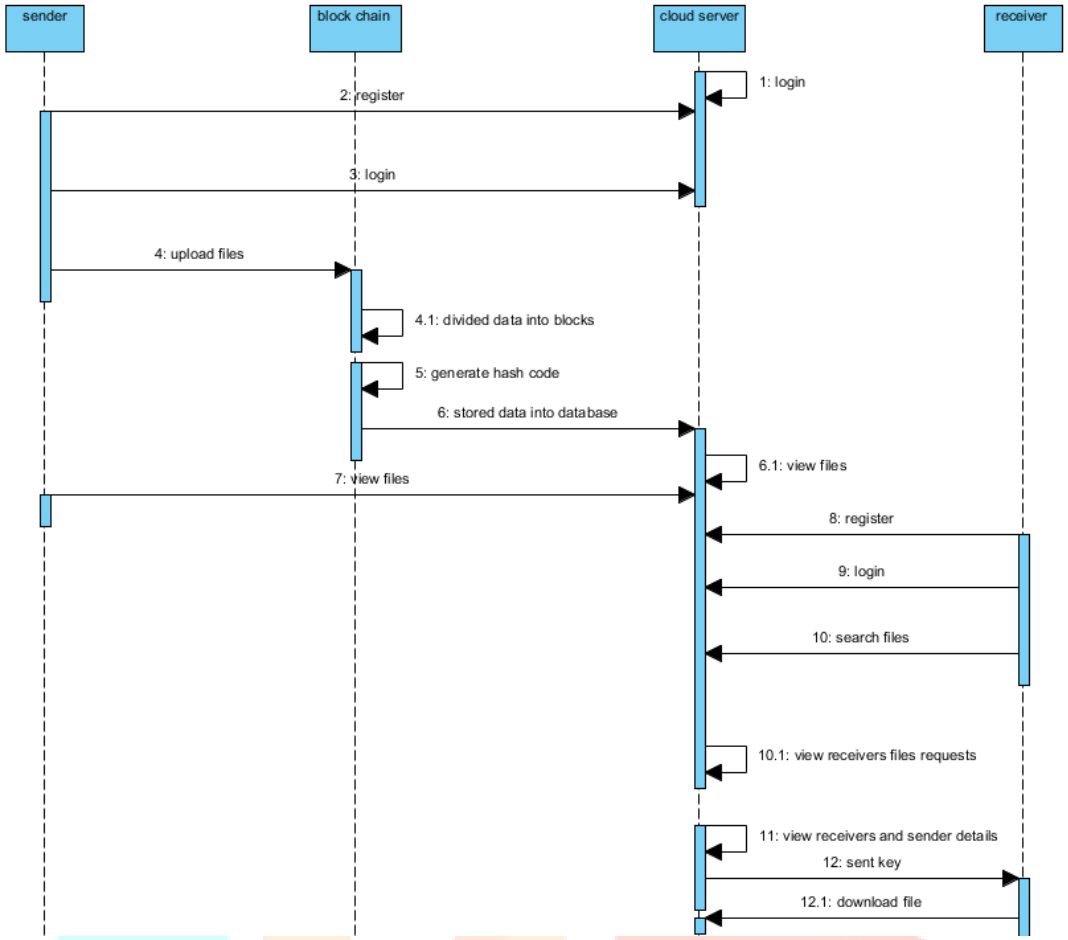

Figure 3: Sequence diagram

V. METHODOLOGY AND ALGORITHM

Round keys are a specific collection of specially generated keys used in the encryption process. They are used on a data array that contains exactly one data block, along with additional operations. the encrypted data. We refer to this array as the state array.

- You encrypt a 128-bit block using the AES procedures below:
- From the cypher key, create the set of round keys.
- Set the block data as the state array's initial value (plaintext).
- The beginning state array should now include the initial round key.
- Carry out nine iterations of state modification.
- Do the eleventh and last state manipulation.
- The encrypted data is copied out as the final state array (ciphertext).3.1Population and Sample.
- The tenth round includes a slightly different manipulation from the other nine rounds, which is why the rounds are labelled as "nine followed by a final tenth round."
- There are only 128 bits in the block that must be encrypted. We first divide the 128 bits into 16 bytes because AES only works with byte amounts. While we say "convert," data is probably definitely already saved in this manner. A two-dimensional, four-row, four-column byte array is used for operations in RSN/AES. 16 bytes of data are used to begin the encryption process.

Four components make up the proposed system: a sender, a receiver, a cloud server, and a block chain. The interactions between each item in the suggested system are depicted in Figure 3.

1) Receiver: The recipient must first register with their information before they can log in using it. Once they have logged in, they may search for files. Once a file is found, they can request to see it in the cloud. If the cloud accepts the request, the sender will get an email with the decryption key to access the file.
2) Cloud Server: The cloud server will log in to the page and verify the senders' and recipients' information. The database's stored files will be seen by the cloud. The key will be given to a specific receiver's email after the cloud has received the receiver's requests.
3) Blockchain: The files are separated into a certain number of blocks that were supplied by the sender, and the divided blocks are then divided into hash codes and recorded in databases.
4) Sender: Sender must first register with their information before they may log in using that information. They can upload the files into the block chain after they have logged in. Following file upload, block chain will carry out block division and hash code creation procedures before storing the data in a database. Sender can access their files when data is saved in the database.

VI. CONCLUSION

A logistics information blockchain data query algorithm based on searchable encryption is proposed in response to the current demand for logistics information at any time. To ensure the reliability and privacy of information, the algorithm combines the benefits and characteristics of blockchain technology with the use of searchable encryption to encrypt and decrypt data. An index list is created for each set of information and may be used to search for the related information once the information has been encrypted by the algorithm and saved in the cloud server. The processes of data insertion and data query, as well as encryption and decryption, are all carefully designed in this study. Lastly, this paper's solution is examined from the perspectives of correctness, completeness, and security, demonstrating the viability of this technique.

REFERENCES

[1] L. Zhang, Z. Y. Zheng, and Y. Yuan, ‘‘A controllable sharing model for electronic health records based on blockchain,’’ J. Automat., vol. 4, pp. 1–14, Nov. 2020.
[2] S. F. Niu, W. K. Liu, and L. X. Cheng, ‘‘Electronic medical record data sharing scheme based on searchable encryption via consortium blockchain,’’ J. Commun., vol. 41, no. 8, pp. 204–214, 2020.
[3] L. G. CH and Q. LI, ‘‘Blockchain data privacy protection mechanism based on searchable encryption,’’ Comput. Appl., vol. 39, no. 2, pp. 140–146, 2019.
[4] H. Qin, Z. Li, P. Hu, Y. Zhang, and Y. Dai, ‘‘Research on point-to-point encryption method of power system communication data based on block chain technology,’’ in Proc. 12th Int. Conf. Intell. Comput. Technol. Autom. (ICICTA), Oct. 2019, pp. 328–332.
[5] J. Sun, L. Ren, S. Wang, and X. Yao, ‘‘Multi-keyword searchable and data verifiable attribute-based encryption scheme for cloud storage,’’ IEEE Access, vol. 7, pp. 66655–66667, 2019
[6] B. Hong, J. Chen, K. Zhang, and H. Qian, ‘‘Multi-authority non-monotonic KP-ABE with cryptographic reverse firewall,’’ IEEE Access, vol. 7, pp. 159002–159012, 2019.
[7] S. Tahir, S. Ruj, Y. Rahulamathavan, M. Rajarajan, and C. Glackin, ‘‘A new secure and lightweight searchable encryption scheme over encrypted cloud data,’’ IEEE Trans. Emerg. Topics Comput., vol. 7, no. 4, pp. 530–544, Oct. 2019
[8] K. Zh and G. Zh, ‘‘A study of ciphertext full-text retrieval based on searchable encryption in cloud environment,’’ Comput. Appl. Softw., vol. 30, no. 4, pp. 35–41, 2017.
[9] L. G. CH and Q. LI, ‘‘Blockchain data privacy protection mechanism based on searchable encryption,’’ Comput. Appl., vol. 39, no. 2, pp. 140–146, 2019.
[10] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, ‘‘Comprehensive study of symmetric key and asymmetric key encryption algorithms,’’ in Proc. Int. Conf. Eng. Technol. (ICET), Aug. 2017, pp. 1–7.