IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 2 - V9I2-1166)
Available online at: https://www.ijariit.com

Ensuring the security of logistics information and data querying using searchable encryption algorithms and Blockchain

T. Sree Lakshmi
lakshmi.nbvm@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

B. Naganandini
naganandinib123@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

B. Manjuula
manjuulab@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

S. Manjunath
manjunath.saddala123@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

G. Rupa
grupareddy727@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

B. Narendra
narendrareddy496@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

ABSTRACT

A searchable and encrypted logistics information block chain data query method is presented to protect the security of logistics information and to query information quickly and efficiently utilizing searchable encryption algorithms paired with the properties of the block chain. The logistics data is split up into many data files, encrypted with an asymmetric technique, and then kept on a cloud server. Each data file is given a keyword index value, which is then uploaded to the block chain. Data updates and queries can be performed at any time with this solution. The project's plan is finally completed with accuracy, completeness, and safety. It offers scheme viability.

Keywords: *Block chain, searchable encryption, asymmetric encryption, logistics information, and data query.*

1. INTRODUCTION

With the fast growth of e-commerce in latest years, the logistics region's enterprise extent has seen an exponential boom sample. Logistics management is turning into more and more informative because of the net industry's brief adjustments, and its strategies, manner, and techniques are evolving towards intelligence. but, there are a number of troubles that still need to be resolved in the back of this trend. Logistics hyperlinks span a huge geographic region and take a long term to finish, making supervision challenging and the elimination of counterfeiting tough. when Satoshi Nakamoto created Bitcoin in 2008, it fast received popularity all around the global. because of its decentralisation, tamper resistance, and traceability, the blockchain generation utilized in Bitcoin has garnered full-size interest from lecturers both locally and the world over.

Blockchain era can deal with the problem of excessive influence in traditional logistics organizations' "vital" enterprise. actual-time viewing and statistics transmission are ensured through the improvement of an open, unified information platform by using a number of events, taking into consideration the capacity to hint back all records additives inside the full statistics chain from production to transit. in the entire facts transmission system, the logistics blockchain is formed via records encryption and consensus verification, thereby making sure the authenticity and transparency of logistics carrier transaction statistics, and ensuring that the facts will now not be tampered with and can be queried and traced to the source. Blockchain can accommodate all users inside the logistics service manner.

Blockchain technology effectively tackles the flaws of traditional tracing methods by utilising its technological components, such as allotted storage, encryption techniques, and timestamps. The many blockchain types can be categorised into public chains, consortium chains, and private chains according on the characteristics of their individual pieces. A blockchain community that is only available to members of the positive group and a small number of 1/3 parties is referred to as a "consortium chain."

A full-size region of study hobby within the logistics quarter has continually been the privateness of logistics facts. the important thing assignment is how to cozy and correctly and quickly query logistical information. Searchable encryption generation can efficiently address this difficulty. the first searchable encryption system that lets in for key-word seek on ciphertext became positioned forth via tune et al. in 2000. The essential technique of using searchable encryption technology is as follows: the user encrypts his very own information and uploads it to the far flung server. whilst the server desires to retrieve the record, the user submits a keyword trapdoor, and the server uses the trapdoor to search for the ciphertext and then returns it to the user. The server won't research whatever about the ciphertext or its key phrases at some point of the entire operation.

In line with the type of encryption, searchable encryption is break up into symmetric searchable encryption and uneven searchable encryption. in their paper, Boneh et al. introduced the concept of characteristic-based totally searchable encryption in addition to the asymmetric searchable encryption scheme. The proxy re-encryption method put forward in is the first scheme wherein information customers can provide different customers the capability to conduct keyword searches.

Those 3 asymmetric searchable encryptions are all searchable. In multi-person contexts, asymmetric searchable encryption is usually used, which is greater relaxed than symmetric encryption. customers' public keys are used to encrypt statistics, and simplest customers with the associated non-public keys can produce search credentials and decrypt the searched ciphertext. is higher ideal for logistics statistics, however has the disadvantage that its algorithm is complicated and its encryption and decryption velocity are both slow.

Decentralization, non-tamperable statistics, and traceability are the 3 key aspects of blockchain era which can be blended in this newsletter, which also indicates a searchable and encrypted logistics records blockchain records query set of rules. The logistical records is cut up up into many information files, encrypted the usage of the asymmetric searchable encryption set of rules, after which stored within the cloud server to address the problem of the uneven searchable encryption technique's gradual encryption and decryption speed. each facts report's key-word index value is extracted earlier than being uploaded to the blockchain, which lessens the load that too much information places on encryption and decryption. statistics updates and queries are always feasible with the set of rules. in this have a look at, some of sub-algorithms are evolved and the encryption and decryption system is designated intensive. in the end, the algorithm's correctness, integrity, and security are examined to illustrate the algorithm's viability.

2. Existing system

Relational and analytical inquiries are desperately needed by the logistics sector, e-finance, e-commerce, and other blockchain applications. Actually A database's primary function in an e-commerce application is to store data that can be retrieved to track transactions, retrieve customer and product information, and maintain inventories. The ability to organise enormous amounts of store data is one of the main advantages of using a database for e-commerce.

A read-only system called an analytical database is used to store historical information on financial variables like sales performance and inventory levels. Business analysts, corporate executives, and other employees use an analytical database to execute queries and generate reports. Recent transaction data from an organization's operational systems is regularly incorporated into the information.A data warehouse or data mart frequently includes an analytical database that is made expressly to serve business intelligence (BI) and analytical applications. This distinguishes it from a transactional, operational, or online database that is used for business applications like order input and transaction processing.

As a result, the current blockchain system's query functionality is incredibly constrained, making it challenging to fulfill the needs of practical second and the active transaction applications. There are some disadvantages in existing system. The Disadvatages are:

- Limited Data Access
- Inefficient
- Less Security

3. Literature survey

The logistical facts may be searched for on the way to affirm that the source of the items is dependable. despite the fact that, it's simple to adjust and fabricate the logistics facts. The conventional approach of looking uses the era based on plain textual content—whether the question person's keywords or the facts data inside the server database are despatched in simple textual content—additionally contributes to main information leakage. due to the widespread hazard to non-public protection and privateness posed by using any malicious server's potential to accumulate facts together with question key phrases and question outcomes of the query person. some academics have recommended a way of searchable encryption and query primarily based on ciphertext to address this issue. To shield consumer privacy and personal protection on this mode, the basics of cryptography are implemented. maximum Blockchain structures use LevelDB , a information garage system constructed for write-in depth programs, as their number one facts garage system, which sacrifices facts examine overall performance for accelerated write performance. but, in real use, the blockchain machine's records writing fee consistent with unit of time is pretty little.

The blockchain device's records writing capacity per unit of time in actual packages, however, is modest. for instance, the modern transaction writing extent of the Bitcoin system is more or less 1 transaction in line with second, at the same time as the Ethereum system presently strategies 7–10 transactions consistent with second. it's miles not possible to reflect LevelDB's benefit in excessive-pace writes.The processing of frequent queries is regularly required due to the growth of apps and the quantity of facts within the blockchain system. The primary bottleneck restricting query performance is the underlying storage machine's read performance, that's insufficient as compared to its excessive write performance.

Unstructured data storage structures based on the key-fee format, like LevelDB, make up most people of the facts garage systems hired via blockchain structures. those systems do not support relational operations for complicated queries; they really offer insertion and querying based totally on Key values. Relational and analytical inquiries are important for blockchain packages in the logistics area, e-finance, e-commerce, and different areas. As a result, the modern-day blockchain machine's query capability is significantly constrained, making it tough to meet the demands of real second-and cutting-edge transaction programs.

To improve query efficiency, a method for including extra indexes to levelDB. The blockchain system's bottleneck, but, will purpose this technique's write function to degrade, and question overall performance can be restrained. In levelDB, which is likewise based totally, counseled a way for including an inner index to create secondary indexes and a question with the important thing cost to increase the effectiveness of tracking and tracing block chains. A useful searchable encryption device based on associated key phrases is proposed in which avoids memorising the places of key phrases with the aid of growing an index of keywords.

Proportion statistics privately and securely without the use of a reliable 0.33 birthday celebration. but, the reality that many key phrases use the identical trapdoor on this scheme ought to lead to hash collision issues.it's far feasible to partly realize the confidentiality of the facts because when the blockchain database is built, a few undeniable textual content continues to be preserved to acquire the identification of the information. In the blockchain database is used to save the encrypted form of personal privacy statistics. A searchable encryption-based solution for protecting blockchain data privateness is placed out in. This approach creates a blockchain transaction sheet the usage of bilinear mapping's mathematical residences and leverages the blockchain to keep encrypted data. A trapdoor is built the usage of the user's searchable encrypted non-public key to search for the provided keyword after the encrypted keyword records has been brought to the transaction order for key-word seek.

A methodology for efficient and comfy massive information retrieval is usually recommended in and is appropriate for encrypted garage. This efficiently guarantees the security of statistics retrieval because there's no facts decryption operation during the whole retrieval process. alternatively, this technique without delay encrypts numerous facts, that's too hard. the usage of blockchain technology, proposes a point-to-point encryption mechanism for data transmitted via power structures.

Traditional communication statistics encryption strategies at the moment are greater stable, however this generation isn't appropriate for eventualities regarding good sized quantities of information. plans that may transfer medical statistics between numerous institutions are provided in both of which use searchable encryption and blockchain generation within the context of scientific treatment. however, the drawback of the 2 systems is that each one of the encrypted facts is saved within the blockchain, adding to the blockchain's storage burden. A multi-keyword search method is proposed in reaction to the issue that most people of searchable encryption handiest allows single-key-word searches. The scope of the quest can be narrowed to exclude useless files, which cuts down on the number of seek calculations. however, this technique ignores the difficulty of facts updating and is beside the point for conditions wherein facts is updated in actual-time, together with with logistics information.

The logistics quarter is an increasing number of being blanketed on a wider scale. the present logistics facts question approach has some drawbacks, which are tested on this paintings at the side of a extra relaxed and effective logistics information query set of rules for large facts volumes. The programme is made extra scalable by way of the algorithm's department of the logistics information into severa facts documents which might be encrypted and kept on a cloud server, along with a keyword index kept on a blockchain. This prevents the cloud server from tampering with the information and lessens the demand on the blockchain's storage. This work develops the corresponding encryption procedure and uses an asymmetric searchable encryption algorithm to encrypt logistics facts. key-word queries are supported for encrypted facts to increase question effectiveness and precision. The extent of logistics information information is good sized and is constantly updated in actual-international software settings. To guarantee the validity of logistical facts, this article suggests a scalable question technique along with blockchain technology.

4. Proposed system

We implement a searchable encryption method that enables keyword searches on ciphertext in the proposed system. The sender encrypts their own data and uploads it to the distant server. When the server wants to recover the file user, they input their keyword data. This is the fundamental application method of searchable encryption technology.

The suggested method encrypts sensitive information using a symmetric encryption algorithm before sending it to a cloud storage platform. The symmetric key k is then encrypted using a quick attribute-based encryption technique. The created ciphertext CT is then posted to the blockchain. It is made up of the access policy CT2 and the key ciphertext CT1, respectively. The integrity of the key ciphertext and access policy are protected by the blockchain because of its decentralisation and tamper-proof capabilities. The computation required for encryption and decryption is significantly decreased through this method, further increasing the effectiveness of the suggested scheme.

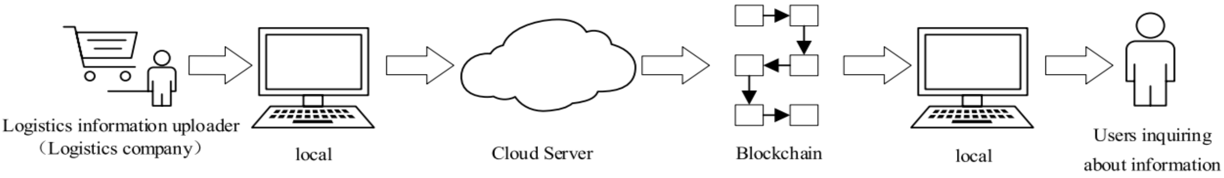


Figure 1. Searchable encryption application process

5. ALGORITHM OF DATA QUERY

A. Summary of the Solution

Because there are so many logistics-related data points, all of the data D is split up into numerous data files, including D1, D2, , and Dn, to increase query efficiency. On the cloud server, the data file D = "D1, D2,..., Dn" is kept. Data is encrypted before being uploaded to the cloud server to preserve data privacy. It is hoped that a technique would be developed that will eliminate the dependency on faith in cloud servers and guarantee that encrypted data cannot be altered. This issue can be successfully solved by the development of blockchain technology. With data integrity and transparency, blockchain is a distributed ledger that may limit illegal access. After being identified and verified by the consensus mechanism, each encrypted document is then stored on the blockchain. A collection of keywords W = W1, W2, , Wm is detected in D before the document is encrypted, and a safe index table I is created. This is done since it is challenging to search for keywords on the encrypted data of the blockchain network. Incorporate the inverted index table I into the smart contract after sending it to the cloud server. Every time you request a keyword search, a trapdoor will be generated, delivered to the cloud server, and then sent to the smart contract.

B. General Defination

This study developed a searchable encryption system based on a logistics blockchain that uses 8 polynomial time algorithms:

π = (KeyGen, SigGen, Build_Index, Adopt, Generate_Trap, Record, Search_Outcome, Dec)

(1) $(K, k_s,(k_{pr} , k_{pu})) \leftarrow KeyGen(1^{\lambda})$: The security parameter is the input for this probabilistic key generation process, which produces the master key K as a result. The pair of asymmetric keys

(2) $Sig \leftarrow SigGen(k_{pu})$: represents the client's public key as input for the deterministic signature generation process, and the MSP module generates the signature Sig that the CA may verify. Clients and peer nodes that take part in the system's work run the algorithm.

(3) $(I, Enc_K\ (D) \leftarrow Build\_index\ (K, D)$: The client is the one who executes the deterministic algorithm. It outputs a secure index I and encrypted documents EncK after receiving a collection of master key K and documents D as input (D). A mapping that can demonstrate whether a document contains keywords is the index table K.

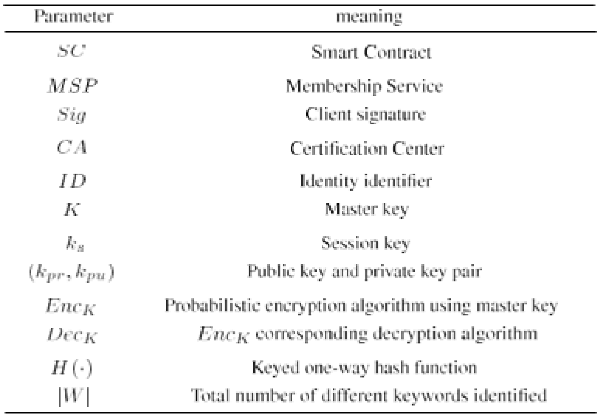
(4) $Embed \leftarrow Adopt\ (Sig, I\ )$: The client is the one that initiates this deterministic algorithm. The algorithm inserts into the smart contract the index table I and the signature Sig as input.

(5) $T_w \leftarrow Generate\_Trap\ (K, k_s, w)$: The master key K, session key ks, and keyword w are inputs into the probability algorithm that is run by the client, and it outputs trapdoors Tw.

(6) $X \leftarrow Search\_Outcome\ (k_s, SC, I, T_w)$: a deterministic algorithm that is executed by the cloud server using a smart contract. The algorithm returns I, which is a set of encrypted document IDs designated as EncK (id (D)), after receiving as inputs an index table I and a trapdoor Tw.

(7) $D_i \leftarrow Dec\ (K, X)$: A deterministic procedure that the client executes that needs the client master key K and the encrypted document identification EncK (id (D)) to decrypt and restore the document id in order to query the associated blockchain data segment.

TABLE 1. **Symbols and description.**



Parameter	meaning
SC	Smart Contract
MSP	Membership Service
Sig	Client signature
CA	Certification Center
ID	Identity identifier
K	Master key
k_s	Session key
(k_{pr}, k_{pu})	Public key and private key pair
Enc_K	Probabilistic encryption algorithm using master key
Dec_K	Enc_K corresponding decryption algorithm
$H(\cdot)$	Keyed one-way hash function
$\|W\|$	Total number of different keywords identified

C. Formula Design

A query based on plaintext is not the same as searchable encryption technology. It is based on encrypted files for query, hence it is required to submit a "tag" equivalent to a plaintext query. With searchable encryption public keys, keywords are encrypted to create the "tag." It is impossible to decrypt encrypted keywords in order to decrypt plaintext, as a result of encryption. Tags created with searchable encryption technology are hence secure in comparison to plaintext tags.

Four entities are included in the algorithm flow this study has designed: a cloud server, a file uploader, and logistics file user and blockchain database (user who queries information). In Figure 1, the implementation of searchable encryption is depicted.

Here are the steps for searchable encryption:
(1) After encrypting the plaintext file and uploading it to the cloud server, the logistics business utilises the key. The keyword is encrypted at the same time and uploaded to the blockchain database using the searchable encryption key.
(2) The user encrypts the keywords that are ready to be queried to create a trapdoor during the query process using the searchable encryption key. While sending the encrypted keywords to the blockchain database, the trapdoor withholds all information about the keywords.

(3) The blockchain database accepts the trapdoor as input and uses the matching algorithm to find the index value that corresponds to the trapdoor. It then uses the index value to query the corresponding file on the cloud server and returns all ciphertext files that successfully match the index value.

(4) After receiving the ciphertext file, the user uses the key to unlock it.A block chain trans- action sheet must be built before data on the chain may be encrypted. A keyword for ciphertext query is added to the blockchain transaction sheet without altering the database's original structure. The purpose of this keyword is to search for encrypted files in the blockchain. It is created by the user encrypting the keyword with a searchable encryption public key.
The data query methodology is broken down into the following steps in detail:

(1) Using a searchable encryption technique, the user creates a trapdoor Tw to access the encrypted data Cw while searching for it with the term w. When searching the blockchain database, Trapdoor $T_{w\,=}$ *Trapdoor (k_{pr} , w)* and sends a search request to the consensus node.

(2)

(2) The consensus node on the blockchain database receives the search request, extracts the trapdoor therefrom, and then runs the searchable encryption algorithm b =Test(k_{pu},C_w,T_w). Match the outcome by testing the kpu, Cw, and Tw. b=1 signifies a successful query, while b = 0 denotes a failed query.
The following steps, in detail, make up the data query methodology:

(3) The user takes the encrypted file containing the keyword w from the transaction sheet that was returned by the blockchain database, decrypts it using the key, and then retrieves the plaintext data file. The user can determine the hash value of the encrypted file to see if the stored medical data file has been altered. The file is correct if the hash value retrieved matches the hash value listed on the transaction sheet. Algorithm 1 is the pseudo code for the

encryption and data query algorithms.

(4)

D. Sub – Algorithm Design

The hyperledger-fabric structure is used as the foundation for this essay. Use MSP to efficiently handle user IDs and verify prospective network peers. MSP components are necessary for hyperledger-fabric. The Certificate Authority (CA), which creates, confirms, and revokes identity-related certificates, serves as the foundation for MSP. Fabric permits the usage of standard interfaces, such as the external CA or Fabric CA API. The two encryption sub-algorithms were created using the same design methodology as Algorithm 2.

(1) KeyGen: Given the security parameter, the key root algorithm creates the master key K, asymmetric key pair kpr, kpu, and session key ks, all of which are shared with the cloud server. K, kpr, kpu (0, 1), and ks are generated by the key root algorithm. This procedure has Algorithm 2 as its pseudocode.

(2) SigGen: Using the client's specific MSP and CA, the method generates a distinct signature using the public key kpu. This procedure has Algorithm 3 as its pseudocode.

E. Design of the data insert algorithm

Encrypted documents can be added to the ledger once the client application and associated blockchain network have been initially set up. Prior to encrypting and storing documents on the cloud server, the client is required to create a secure index table I. The index Boolean I is a mapping that displays whether or not there are keywords in the text. The keyword cannot be determined, and this is the only information that can be deduced from I. Once the index table I has been properly constructed, the client encrypts the document D with the help of the master key K before sending the encrypted document D and the index table I to the cloud server for recording in the ledger. For access verification and granting, the client sends the MSP a copy of its signature. The algorithm for inserting data is as follows:

Create the _Index: Using the algorithm suggested in [20], the client creates the index table I. The algorithm employs the cryptographic hash function H 0, 1 W 0, 1 L, where L is the length of the output. The client's master key K is hashed by the keyed hash function H using the client's master key. In order to map probability trap gates, the approach is also dependent on the modular inverse feature. By default, the index table displays the frequency of encrypted keywords that were used in documents and led to statistical analysis assaults. This problem is avoided by the suggested approach, which only uses shokeywords in the document and hides these values to lessen the danger of attack. If there are encrypted messages, the pseudo code for this process is Algorithm 4.ws.

(1) Adopt: The algorithm embeds the updated index table acquired from the Build Index algorithm into the smart contract's query function given the index table I and signature. This procedure has Algorithm 5 as its pseudocode.

(2) Record: The algorithm adds the documents to the ledger after receiving the encrypted document set D. In order to start the consensus mechanism, the client must first authenticate using MSP. Add the transaction node to the ledger when it has been verified. This is required to maintain trap doors, store encrypted documents, and retrieve old search results. This procedure's pseudo-code is designated as Algorithm 6.

F. Design of Keyword Search Algorithm

The customer must create a probability trapdoor for keyword search. The generation of the trapdoor requires the client's master key and the customer can additionally submit key phrases for reference search since only authorised individuals can generate a meaningful trapdoor. Because a new trapdoor can be constructed using the same keyword search and sent to the cloud server to search on behalf of the client, probabilistic trapdoors can withstand attacks in a differentiated way.

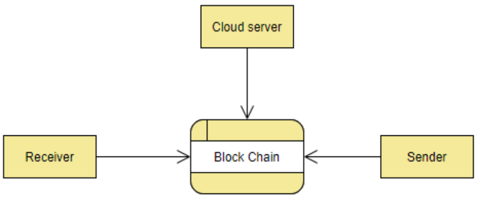
In order to find the encrypted document identification EncK (id (Di)) containing the keyword, the client application uses the query command to reach the cloud server. It then notifies the client of the search result and initiates the Get operation using the smart contract of the trapdoor. Through a consensus process, the trapdoor is connected to the ledger. The necessary encrypted document is then directly obtained from the blockchain network, where it may be decrypted by the client with the master key.

(1) Generate Trap: The client creates a probability trapdoor in order to search for keywords on encrypted documents kept on the blockchain. Make the trapdoor probabilistic by using a probabilistic asymmetric encryption technique. Similar to the Build _Index technique, the algorithm likewise employs a keyed hash function. The trapdoor Tw is sent to the smart contract so it can search on the client's behalf. Algorithm 7 serves as the process's pseudocode.

(2) Search Outcome: The method is built into the smart contract and is used to communicate probabilistic trapdoors and search on the client's behalf. The item d Hks c a1mod P is calculated and recognised by the cloud server. The smart contract gives the client of the needed block on the network the document identifier after successfully identifying the column. The Record algorithm is once more activated because the search is likewise documented as a transaction. This procedure's pseudo-code is designated as Algorithm 8.

(3) Dec: To find the block holding the desired document, the client decrypts the encrypted document identifier. The required papers can now be obtained by the customer straight from the blockchain network. This procedure's pseudocode is designated as Algorithm 9.

The logistics chain querying logistics information process employing searchable encryption techniques is designed in this section based on the logistics scene combined with Blockchain. Then, the relevant encryption and decryption methods are explained. An algorithm for data insertion is created to guarantee that the logistics data may be updated on the chain in real time. The keyword search algorithm is described lastly in accordance with the properties of the searchable encryption algorithm.



Context Level Daigram

6. ANALYSIS AND PROOF OF ALGORITHMS

This document satisfies ciphertext security, keyword security, and secure query information requirements.
Principle 1: Correctness The user can obtain the accurate clear text of logistics information if the cloud server, user, and smart contract honestly execute this algorithm.

Proof: Assume that the logistics company possesses the plaintext D of the logistics information data, the keyword set W, the identifier ID of the logistics information data file, the encryption key ks, the asymmetric key kpr, the kpu to construct the index, and the other keys. Upload the logistical data's ciphertext, ED DEnc, to the cloud server (ks, D). Uploading the index I to the cloud server requires running the Build _Index algorithm.

E. D. Enc (ks, D). Put the index I online on the cloud server by running the Build _Index algorithm. The logistics business randomly chooses xi I = 1, 2, • • •, t 1) and calculates y (x) = k2 + a1x + a2x2 + • • • + at1xt1mod q when n users submit a search request. It also randomly chooses si I = 1, 2, • • •, n) and the coefficient bi I = 1, 2, • • •, t 1) and calculates Send y (xi), v (si) I 1, 2,, n) to the corresponding user, and then record the hash value of y (xi), v (si) and the value of xi, si in the blockchain. . It takes two steps to search for logistical data that contains the term w when there are users that meet the threshold (specified as t) and want to cooperate:

Phase 1: the search To the blockchain, the user submits his key share y (xi)r I 1, 2,, and t) and keywords w.
(1)The key k2 for creating the index is equal to the value of k2r calculated by the smart contract according to the Lagrange interpolation polynomial since the user and the smart contract honestly carry out this scheme. Following that, provide the user the determined search credentials T r (sw, tw). Given that the cloud server implements this solution honestly and parses the search credentials T r, the user submits those credentials to the cloud server (sw, tw).

If the index I contains the keyword w, the cloud server can locate the matching EIDw according to sw, decrypt it to obtain IDw IDDec (tw, EIDw), and then return the appropriate ciphertext EDw of the logistical information including the keyword to the user according to IDw.

(2) phase of decryption: The user provides the blockchain his key share v (si)r I 1, 2, t) and cipher-text EDw of logistical data when he wishes to decrypt. Since both the user and the smart contract accurately execute this process, the smart contract's determination of the encryption key k1 using the Lagrangian interpolation polynomial, or k1r, results in Drw DDec DEnc (k1, Dw), k1r DDec ((k1, Dw), k1) Dw. So that the user can receive the right plaintext of logistics information data, the smart contract transmits Dw to the user.

The second principle is that logistical information data must be confidential and accurate.
Proof: Before being uploaded to the cloud server, the logistics data is encrypted. The cloud server is somewhat trustworthy, but it will nonetheless carry out the user's request and is highly curious in the user's personal information. The cloud server is unable to access the decryption key in the technique presented in this work because all ciphertext files are kept there. As a result, the data's privacy can be ensured because the file cannot be decoded. The client encrypts the data using the user's public key. Kpr realises the confidentiality of logistics information because only the user has the ability to decode it since it is the user's private key. The data in the blockchain is also unchangeable. The data cannot be updated if it has already been added to the chain.

Proof: A is a polynomial time adversary, denoted as A A0, A1, and Aq 1, given the safety parameters (q N). When q 0 is reached, the adversary outputs D0, D1, and stA0 in accordance with the safety settings. (1) The challenger C then uses the KeyGen algorithm to generate the key kpu, kpr. The opponent A1 receives EDb and an index Y equal to the true index Ib from the challenger C after it randomly chooses the values b 0, 1, and executes algorithm DEnc on Db.
The indistinguishability of ciphertext is satisfied since stA0 does not contain kpu, making it impossible for the adversary to tell the difference between the true ciphertext and EDb. Similarly, The adversary cannot differentiate between the index Ib and the genuine index since stA0 does not contain kpr, which satisfies the index's requirement for indistinguishability.

(2) When q = 1, the adversary A1 sends the search credentials Tb,1 swb,1, and twb,1 to the adversary A2 along with the outputs w0 and w1 i.

Since the adversary cannot tell Tb,1 from the actual search voucher because stA0 does not contain kpu, this satisfies the search voucher's requirement for computational impossibility based on the collision resistance of the hash function. The first theorem explains the algorithm's correctness; the second theorem analysis demonstrates the algorithm's completeness, i.e., that it won't damage the original data; and the third theorem demonstrates from the standpoint of adaptive indistinguishability. The algorithm developed in this research is efficient and practicable for enhancing algorithm security.

7. CONCLUSION

A logistics information blockchain data query algorithm based on searchable encryption is proposed in response to the current need for logistics information at any time. In order 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 collection of information and may be searched using keywords. The algorithm first encrypts the data before storing it in the cloud server and retrieving it using keywords. This document includes a detailed design of the data insertion and data query processes as well as the encryption and decryption processes.

8. REFERENCES

[1] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Eletronic CashSystem.[Online].
[2] Q. F. Shao, ‘‘Blockchain: Architecture and research progress,’’ Chin. J. Comput., vol. 425, no. 5, pp. 3–22, 2018.
[3] Y. Yuan, X. Ni, S. Zeng, and F. Wang, ‘‘Blockchain consensus algorithms: The state of the art and future trends,’’ Acta Automat. Sinica, vol. 44, no. 11, pp. 2011–2022, 2008.
[4] D. X. SONG, D. WAGNER, and A. PERRIG, ‘‘Practical techniques for searches on encrypted data,’’ IEEE Symp. Secur.

Privacy., Oct. 2000, pp. 44–55.
[5] J. Li, C. F. Jia, Z. Liu, J. Li, and M. Li, ‘‘Survey on the searchable encryption,’’ J. Softw., vol. 26, no. 1, pp. 109–128, 2015.
[6] D. Boneh, ‘‘Public key encryption with keyword search,’’ in Proc. Int. Conf. Adv. Cryptol., 2004, pp. 506–522.
[7] Q. J. Zheng, S. H. Xu, and G. Ateniese, ‘‘VABKS: Verifiable attribute based keyword search over outsourced encrypted data,’’ in Proc. IEEE Conf. Comput. Commun., Apr. 2014, pp. 522–530.
[8] J. Shao, Z. Cao, X. Liang, and H. Lin, ‘‘Proxy re-encryption with keyword search,’’ Inf. Sci., vol. 180, no. 13, pp. 2576–2587, Jul. 2010.
[9] 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.
[10] Q. Wang, P. He, and T. Nie, ‘‘Survey of data storage and Query techniques in blockchain systems,’’ Comput. Sci., vol. 45, no. 12, pp. 12–18, 2018.
[11] X. Liu, X. Yu, X. Ma, and H. Kuang, ‘‘A method to improve the fresh data Query efficiency of blockchain,’’ in Proc. 12th Int. Conf. Measuring Technol. Mechatronics Autom. (ICMTMA), Feb. 2020, pp. 823–827.
[12] Y. P. Luo, N. T. Zhu, C. W. Mao, and J. X. Ch, ‘‘A practical searchable encryption scheme based on connection keywords,’’ Comput. Eng., vol. 46, no. 2, pp. 175–182, 2020.
[13] N. Zh and Z. Sh, ‘‘Mechanism of personal privacy protection based on blockchain,’’ Comput. Appl., vol. 37, no. 10, pp. 2787–2793, 2017.
[14] 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.
[15] 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.
[16] 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.
[17] 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.
[18] 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.
[19] 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.
[20] 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.
[21] F. Gao, M. Shen and L. Zhu, “Research review on blockchain privacy protection,” Computer Research and Development, vol. 54, no. 10, pp. 2170–2186, 2017.
[22] S. Noether, A. Mackenzie and Research Lab T. M., “Ring confidential transactions,” Ledger, vol. 1, pp. 1–18, 2016.
[23] J. K. Liu, V. K. Wei and D. S. Wong, “Linkable spontaneous anonymous group signature for ad hoc groups,” in Australasian Conf. on Information Security and Privacy, Berlin, Heidelberg: Springer, vol. 3108, pp. 325–335, 2016.
[24] Y. Chen, A. Haseeb, C. Li, J. Li and G. Xu, “A new anti-quantum proxy blind signature for blockchain-enabled internet of things,” Computers, Materials & Continua, vol. 61, no. 2, pp. 711–726, 2019.
[25]A. Chiesa, C. Garman and E. B. Sasson, “Zerocash: Decentralized anonymous payments from bitcoin,” in IEEE Symp. on Security and Privacy, 2014. CMC, 2021, vol.66, no.1 883
[26] A. Chiesa, D. Genkin and E. B. Sasson, “Snarks for c: Verifying program executions succinctly and in zero knowledge,” in Annual Cryptology Conf., Berlin, Heidelberg: Springer, pp. 90–108, 2013.
[27] C. Decker and R. Wattenhofer, A fast and scalable payment network with bitcoin duplex micropayment channels. In: A. Stabilization, Safety, and Security of Distributed Systems, vol. 9212. New York: Springer Verlag, 3–18, 2015.
[28] I. Bentov, R. Kumaresa and A. Miller, “Sprites: Payment channels that go faster than lightning,” Available https:// arxiv.org/abs/1702.05812.
[29] L. Alshenibr, F. Baldimtsi and E. Heilman, “TumbleBit: An untrusted bitcoin-compatible anonymous payment hub,” Network & Distributed System Security Symposium, 2017.
[30] M. Green and I. Miers, “Bolt: Anonymous payment channels for decentralized currencies,” in Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security, ACM, pp. 473–489, 2017.