IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE THE LOGISTICS INFORMATION DATA USING BLOCK CHAIN

B.Malathi(M.Tech)
Department of CSE,
School of engineering and Technology,
Sri Padmavathi Mahila Visvavidayalayam, india,
(women's University),
Tirupati.

A.Supriya, PhD.
Asistant Professor,
Department of CSE,
School of engineering and Technology,
Sri Padmavathi Mahila Visvavidayalayam, india,
(women's University),
Tirupati.

ABSTRACT

A searching and encrypted logistic informational blockchain data query method is presented to ensure the safety of logistics information and to query content quickly and efficiently utilizing's searchable encryption algorithms paired with the properties of the block chain. The logistical data is first separated into different data files, then encrypted using an asymmetric searchable encryption technique and saved in the cloud server. Each information keyword index is extracted and published to the blockchain. This solution is available at all times. Data can be updated and queried.The research directs in-depth on smart contract technology in algorithm to make query efficiency more better .At last the scheme of this article is solve errorless,completeness and safety .It proves scheme feasibility.

1.INTRODUCTION

1.1 General:

The logistics technology and manufacturing volume has seen an accelerated growth trend during the period, thanks to the rapid rise of e-commerce. Because of the dramatic modifications on net business, the balancing on logistics is extremely informative, and The methods, averages, and strategies used in logistics management and operations are getting increasingly sophisticated. However, there are other issues to be addressed in order to continue this development. Because logistics ties span numerous places and have large time spans, tough supervision, and hard imitation to eradicate. Satoshi Nakamoto created digital currency in 2008, and the virtual money quickly gained popularity around the world. Because of its decentralization, tampering tolerance, and tracking, the blockchain technology in Bitcoin has piqued the interest of academics both at home and abroad. The problems of excessive control in logistics services enterprises ``central'' management can be solved using blockchain technology. Real-time monitoring and information transfer are secured by the construction of a transparency-bind information platform by numerous parties, allowing all sections of the chain from production to transport to be realized. Can be traced back in time. The block chain network of logistics is created data encryption and verification of make sure throughout the entire data transfer process, ensuring the validity and the transactional transparency of logistics services details, as well as verify that the info will not be interfered with, and might even be questioned and verified back to its original form. Using technological attributes as dispense repository, data encipher, time stamping & block chain successfully overcomes the pain points of traditional tracing solutions. According to the features of their participants, blockchains can be classified as public chains, collaborative chains, or private chains. The consortium chain is a blockchain system, only certain associates of a group and a few other parties have access to.

1.2 PROBLEM DEFINITION:

This application used to Encrypts personal info and uploads it to a cloud service for storage using a symmetric encryption technique. The symmetric key k is then encrypted using a fast attribute-based encryption technique. The created cipher - text CT is then posted to the network, consisting of the key cipher-text CT1 and the access policy CT2. The blockchain is utilized to protect the integrity of the key cipher-text and access policy due to its decentralized and tamper-proof properties. Reduces computation operations on encryption and decryption more effectively.

1.3 OBJECTIVE OF THE PROJECT:

The goal of this assessment is to conduct a search for this and assure the use of blockchain with logistical data. The data query approach for obtaining the confidentiality of logistics data and querying it quickly and effectively utilising searchable strong encryption combined with blockchain capabilities. Initially, The logistical data is separated into distinct papers, encrypted with an uneven searchable encryption method, and thereafter saved on a cloud administration. A watchword track esteem of each data document is recovered and transmitted to the blockchain. This assistance is available anytime and whenever query data is updated.

2.LITERATURE SURVEY

SURVEY ON LOGISTICS INFORMATION BLOCKCHAIN:

Yibo Sun1, Xiaofang Li1, Furu Lv, And Bing Hu . IEEE, 2021.An accessible and scrambled logistics data blockchain information query strategy is introduced to secure the integrity of logistical data and to query data quickly and effectively utilising easily accessible encryption computations that are compatible with the blockchain's features First and foremost., the calculated information is isolated into various information documents, encoded with a deviated accessible encryption method, and saved money on the cloud server. Every information document's catchphrase file esteem is separated and distributed to the blockchain. This arrangement is appropriate without warning. Information is refreshed and questioned. At last, assess the rightness, fulfilment, and security of this current article's plan, which exhibits its plausibility. The innovation considered by the client and the creator is blockchain dependent on accessible encryption.[1].

Liangming WenLili Zhang, 2019.Blockchain is thought to be the fundamental development that will lead to the transition from the Information Internet to the Value Internet. A growing number of organisations are investigating the commercial applications of blockchain, and one of the most hotly debated topics is how to use blockchain in data management. This article is based on blockchain and provides a detailed analysis of its middle sections, progressions, and applications. Then, it brushes over the issues that data executives are concerned about, such as quality, security, and sharing, and separates the application benefits of blockchain development in the data industry, and advances a data community-oriented administration model ward on blockchain, which has the properties of decentralisation, total assistance, customised execution, and non-tamperability. Client validation is covered by the model. information confirmation, information logging, information sharing and different cycles, and is outfitted with an information-the executives motivator framework, which can accomplish advantageous, secure and quick information on the board. Applying blockchain innovation to information the executives can additionally work on the adequacy of information the board and work on the nature of information, and establish a positive information sharing environment. There are different types of life cycles involved in the technology of block chain.[2].

D. X. SONG, D. WAGNER, and A. PERRIG. Oct. 2000,pp .To reduce security and insurance risks, it is interesting to store data on data mail servers, such as mail servers and record servers, in scrambled organisations. Regardless, this generally implies that one should forego esteem in exchange for security. For instance, to recuperate just reports containing explicit terms, It was previously unknown how to allow the data storage server to process the request and respond to the enquiry without jeopardising data security. We present our cryptographic methods in this work.methodologies to the issue of checking out mixed information and deal wellbeing confirmations for the succeeding crypto systems. Our methodologies give various quick benefits.[3].

Q. J. Zheng, S. H. Xu, and G. Ateniese, ‘‘VABKS: 2014**.** It is not uncommon for employers to shift their data to the cloud now. Because the cloud cannot be totally trusted, the readdressed data should be jumbled. This, however, raises a number of concerns, including how an information proprietor should grant searchcapabilities to data customers. Again how many authorised data customers look through aninfo proprietor re-appropriated encrypted text? How can data consumers be certain that thecloud consistently carried out the search method for their advantage? In response to thesequeries, we offer an ingenious crypto organization known as evident strong qualitywatchword search (VABKS). The approach empowers a data consumer whose credentialssatisfy a content proprietor entryways control strategy to (I) seek over the info proprietorre-appropriated encoded data, (ii) reassess the tedious endeavour actions to the cloud, and(iii) confirm if the data center has consistently performed the hunt functions. We formallyoutline VABKS regulatory standards and present a development that meets them. Theoperational evaluation reveals that the offered plans are practical and deployable. Whileencrypting the content, the researcher discusses the method known as VABKS[4].

Summary:

- ➢ In this paper, cryptographic approaches to the problem of mixed data analysis. Our solutions are provably safe and provide encryption with a proven secret. They also accept saved queries, so the client can ask the untrustworthy server to search for a peculiar term.
- ➢ Based on searchable feature encryption, this paper proposes a blockchain data privacy safe control approach. It solves the issue of privacy infringement in common transactions by integrating property encryption with linear secure transfer. The verification nodes handle the user's access control, avoiding the risks of security and sending keys.A delivery gives k-namelessness assurance in the event that the data for every data
- ➢ Individual contained in the delivery can't be recognized from at minimum k-1 people. This paper likewise analyses re-distinguishing proof assaults that can be acknowledged on discharges that hold fast to k obscurity.

2.1 ANALYSIS ON LITERATURE SURVEY

S.NO	TITLE	DESCRIPTION	KEY IDENTIFIED
1	Research on Logistics Information Block chain Data Query Algorithm Based on Searchable Encryption[1].	This present paper's answer is explored according to three correctness:rightness, completeness, and security, showing the achievability of the methodology. The subsequent stage in the review interaction will be to act inside and out research on the brilliant agreement innovation in the calculation to expand query effectiveness.	The high velocity compose benefit of LevelDB can't be reflected. With the increment of information in the blockchain framework and the extension of uses, incessant questions regularly should be handled. The compose execution of the fundamental stockpiling framework is inordinate yet the read execution is deficient, which has turned into the principle bottleneck that cutoff points question execution.
2	Application of Block chain Technology in Data Management: Advantages and Solutions[2].	Block chain is viewed as the critical innovation to lead the transition from an information-based internet to a value-based internet. How to apply blockchain in information the executives has become one of the focal points of conversation. The model covers client validation, information confirmation, information logging, and information sharing and different cycles.	Blockchain innovation gives a significant change in outlook in business process streamlining, information trade and interoperability in related enterprises, and furthermore gives another way for information to the board. the key advancements that make up the blockchain, attempting to respond to the subject of how to utilize the upsides of blockchain innovation to compensate for the inadequacies of information the executives.

3	Homomorphic Encryption and Network Coding in IoT Architectures: Advantages and Future challenges[7]	Network Coding can help distant enterprises improve their security & efficiency. Homomorphic Encryption can be used to run computations on the cloud while ensuring data security. The advantages of NC and HE are highlighted across the entire spectrum of cloud-based IoT platforms.	The execution of NC all through the engineering can decrease the whole framework's inactivity. It improves the accompanying cycles: interchanges multi-cloud information transfer and download through the WSN, as well as information recovery and unravelling. In spite of this, as referenced over, these plans can be adjusted to existing IoT conventions.
4	VABKS:Verifiable attribute based Keyword search over outsourced encrypted data[4].	Because of cloud can indeed be totally believed, the re-evaluated data should be jumbled. We suggest an ingenious encrypted scheme known as obvious quality based watchword search (VABKS). The approach allows an informational client to look through the data proprietor re-appropriated encrypted data.	It is now commonplace for data controllers to subcontract their data to the cloud server. Because the cloud can indeed be wholly believed, the information that is outsourced should be encrypted. It raises a number of concerns, including how a data controller can offer search functions to information consumers. So the biggest disadvantage is because there is no substantial proof on putting your data in the cloud, implying that the data saved in the cloud is not entirely trustworthy.

3. OVERVIEW OF PROPOSED SYSTEM

3.1 INTRODUCTION:

This scheme utilizes a symmetric encryption algorithm on private data to encrypt. Cloud platform used as storage for uploads. For encrypting the symmetric key K, a fast attribute-based encryption algorithm is used. The ciphertext CT which is generated consists of ciphertext key CT1 and access policy CT2 uploads to the blockchain.The study focuses on using an algorithm that uses smart contract technology to improve query efficiency..At last the scheme of this article is solve errorless, completeness and safety. The presence of decentralization and tamper-proof, protect the integrity of ciphertext key and access policy in blockchain.

3.2 ARCHITECTURE OF THE PROPOSED SYSTEM:

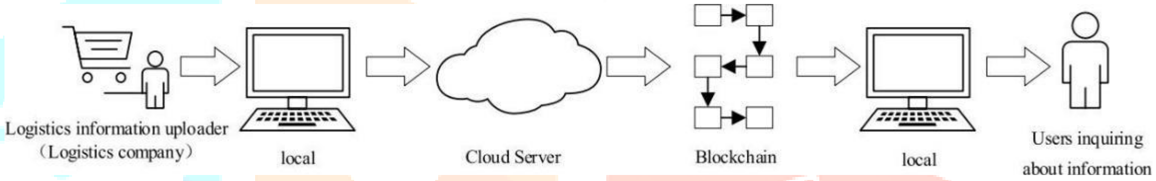


Fig 3.2 Architecture of Proposed System

In the above graphic, the essential elements or activities are done by blocks connected by lines that demonstrate the relationship of the squares. The square graph is a representation of the framework's execution; however, because it is a representation of this course of action, it exposes less of the framework. The programme seems as if a UI completely stays alive on a data set known as SQLite that works with Android SDK and does not require any additional setup. This is the database that is used to provide spring and recovery refuge advice.

4. ALGORITHMS

4.1 Hashalgorithm:

A hash is similar to a thumbprint . A cryptographic hash algorithm is used to generate each block hash (SHA 256). As a result, differentiating each block in a blockchain framework is no longer a challenge. The moment a blocks is created, it automatically appends a hash, and any advancements performed in a block also impact the variance in a hash. Hashes, simply said, aid in distinguishing any progressions in blocks. The hash from such a previous block is the final component within the block. This sets off a chain of blocks and is the main ingredient underlying the integrity of the blockchain system. For example, block 45 relies on block 46.

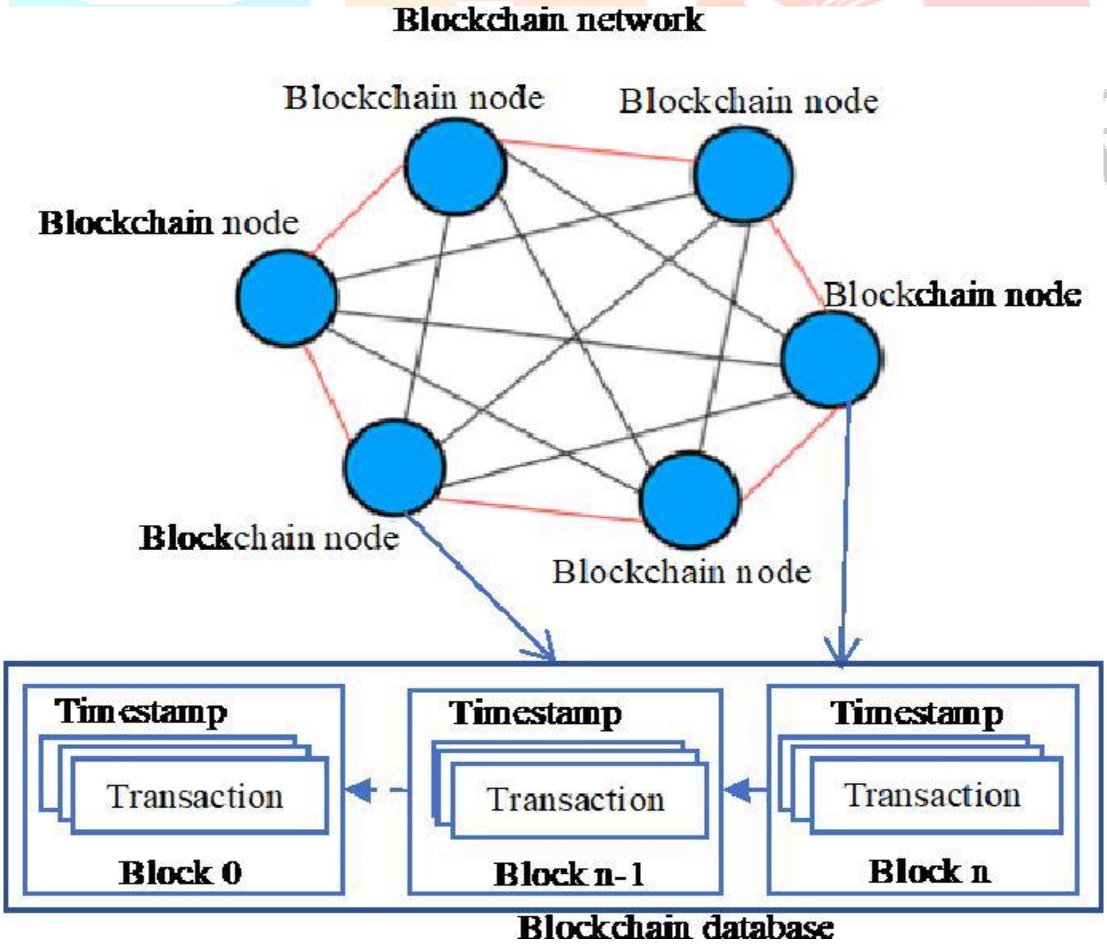
4.2 Encryption & Decryption Algorithm:

The encryption procedure employs a set of round keys, which are uniquely derived keys. These, along with additional procedures,are applied to a data array that contains exactly one encrypted data block. The state array is the name for this array.

Perform the following aes encryption steps for a 128-bit block:

- ➢ Make a succession of circular keys from the cypher key.
- ➢ Fill the state array with the block data (plaintext).
- ➢ Add the initial round key to the starting state array.
- ➢ There are a total of nine rounds of state manipulation required.
- ➢ The eleventh and final state manipulation phase should be completed.
- ➢ Make an encrypted duplicate of the final state array (ciphertext).
- ➢ For operations, RSN/AES uses a two-dimensional byte array with four rows and four columns. At the start of the encryption, there are 16 bytes of data.

4.3 FLOW OF THE ALGORITHM



5.CONCLUSION

The goal of this paper was to derive key elements that would ensure the security of logistics data while also allowing users to query data quickly and efficiently using searchable encryption methods and blockchain characteristics. In response to the present demand for logistics data and information, a blockchain data query technique based on searchable encryption has been developed. It incorporates blockchain technology's features and qualities, as well as searchable encryption for data encryption and decryption, to ensure dependability and confidentiality. The method first encrypts the data, which is then stored on a cloud server. An index list is created for each collection of data, and keywords can be used to discover relevant data. The techniques for encryption and decryption, as well as data insertion and inquiry, are all detailed in this paper. Finally, the research focuses on using smart contract technology to improve query efficiency in algorithms.

6.REFERENCE

[1] Yibo Sun1, Xiaofang Li1, Furu Lv, And Bing Hu "Research on Logistics Information Block chain Data Query Algorithm Based on Searchable Encryption".Special Section on Blockchain Technology: Principles and Applications. IEEE, 2021

[2] Liangming WenLili Zhang, ''Application of Blockchain Technology in Data Management: Advantages and Solutions,'' Springer. 2019

[3] D. X. SONG, D. WAGNER, and A. PERRIG, ''Practical techniques for searches on encrypted data,'' IEEE Symp. Secur. Privacy., Oct. 2000,pp. 44–55

[4] Q. J. Zheng, S. H. Xu, and G. Ateniese, ''VABKS: Verifiable attribute based Keyword search over outsourced encrypted data,'' in Proc. IEEEConf. Comput. Commun., Apr. 2014, pp. 522–530.