EasyChair Preprint

№ 9918

Studying Logistics Data Using a Searchable Encryption-Based Data Query Algorithm for Blockchain

Venkatesh Gorantla, Jayanth Sai Bhogi Reddy,
Ravi Sankar Keerthi, Sai Ganesh Gurram and
T Dhiliphan Rajkumar

March 31, 2023

Studying Logistics Data Using A Searchable Encryption-Based Data Query Algorithm For Blockchain

G. Venkatesh, B. Jayanth Sai, K. Ravi Sankar, G. Sai Ganesg, and T. Dhiliphan Rajkumar
CSE, Kalasalingam Academy Of Research And Education, Madurai, India

Vgorantla81@gmail.com
Jayanthsai8172@gmail.com
Keerthiravisankar123@gmail.com
Saiganeshgurram0@gmail.com
t.dhiliphan@klu.ac.in

***Abstract*—To ensure the safety of delivery channels and view data quickly and efficiently using searching strong encryption and the advantages of the blockchain, a searching and protected logistical info blockchain hive query algorithm is offered. The logistics data is divided up into several data files, subsequently saved on a cloud platform after being encrypted using an asymmetric method. The keyword index value of each data file is obtained and submitted to the blockchain. This treatment is always accessible. data search and updating. In order to prove the article's feasibility, take into account if the strategy is correct, comprehensive, and secure**

***Keywords*— Encryption, Feasibility, Logistics, Data Query, Counterfeiting, Cryptography.**

I. INTRODUCTION

The logistics division has shown a huge popularity tendency in recent years due to the quick expansion of e-commerce. Logistics supervision including working methods and the plan is slowly becoming more clever as a result of the Internet industry's rapid developments, which have made logistics management more and more informative. But other issues need to be resolved underlying this trend. Logistics linkages span a large number of locations and have longer transit times, making oversight challenging and the elimination of counterfeiting challenging. Bitcoin was created in 2008 by Satoshi Nakamoto, and virtual money quickly spread around the globe. The blockchain technology behind Bitcoin has attracted a lot of interest from academics both locally and globally. Blockchain is used to address the issue of superior authority in the "central" structure of traditional logistics organizations. Real-time and data transmission is made feasible by the development of an open, consistent information platform by several parties, which enables the ability to track all information components throughout the whole information chain from production to travel. Blockchain can able to provide all website visitors in an integrated logistics process. During the whole data communication time, the logistics ledger is formed through cryptographic protocols and general agreement verification, making sure the truthfulness and freedom of logistics log entries and the data will never be messed with and can be enquired about, tracked to its user. Blockchain technique successfully addresses drawbacks for conventional tracing types using their technological capabilities, like cloud databases, and timestamps. A blockchain network known as the consortium chain is solely accessible to certain members of an organization and a small number of third parties.

Devolution, non-tamper able info, and traceability are the three key aspects of blockchain technology that are combined in this paper, which also suggests an accessible and protected logistics info blockchain database query method. To address the issue of sluggish encryption. The logistical data is separated into many data files, encrypted using the asymmetrical searching encryption technique, and afterward stored in the cloud server to increase the speed of decrypting. Each data document's keyword scale is removed before being posted to the blockchain, which lessens the

pressure that too much data places on both encryption and decryption

II. Literature review

2.1 L. Zhang, Z. Y. Zheng, and Y. Yuan, "A controlled sharing paradigm for electronic medical records based on blockchain," J. Automation., volume. 4, pp. 1–14, November 2020.

The Inter Terrestrial 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 expenditures in blockchain while ensuring medical data'.

2.2 S. F. Guo, K. Liu, X. Chengi, "Electronic health records information transport strategy relying on cryptography algorithms through blockchain," Journal of Communications, vol. 43, no. 2, 2020, pp. 207–219.

Because the data on the blockchain is unchangeable, its security is increased. We propose a blockchain system used to share electronic medical record data that enable third-party data users to share patient data without invading patient privacy. We first provide a system model for the strategy. A consortium blockchain and a private blockchain are both used to build the system. The patient's medical history is stored on a private blockchain (DR). Secure indexes made up of DR keywords are kept on the consortium blockchain. Diagnostic data and keywords are stored as encrypted ciphertext data. To protect keyword searches on the consortium blockchain, we secondly employ public encryption with keyword search (PEKS) technology.

2.3 Q. LI and L. G. CH, "Blockchain information safety technique based on encryption," Computer. Technology., volume. 33, no. 5, pp. 147–152, 2017.

Collusion issues may be resolved by coupling the secret crucial part with the arbitrary user node identification in the blockchain. Additionally, using searchable encryption, authorized individuals may instantly examine and monitor transaction information.

2.4 H. Qian, Li, Zhao, "Technique for transmission line interaction statistics based on blockchain technology," in Proc. 14th Intelligence Computer Technology, October 2018, pp. 326-333.

An encryption technique like data used in system communications related to blockchain technique is being researched and developed to address the lack of reliability of conventional communication data encryption methods. The design technique uses blockchain technology's decentralization and consensus mechanism to create the public access control scheme by the asymmetric key encryption concept.

2.5 J. Du, L. Liu, S. Wang, and X. Yao, "Multi-keyword navigable and evidence verifiable feature encryption system for cloud storage," IEEE Access, edition. 7, pp. 655–667, 2019.

It is a fundamental necessity in a data-sharing system for a user to be able to execute keyword recovery for encrypted documents kept in the cloud. Even though the fact that data security and retrieval capabilities may be provided by typical searchable encryption technology, certain major difficulties mustard are certain major difficulties that must also be taken into account. First off, the majority of 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 about certain terms, yet his characteristics may frequently change. Thirdly, the central server is not always trustworthy and occasionally gives a small number of inaccurate search results.

2.6 R. Mustafa, F. Rahul, M. Raja, & D. Glack, "Novel safe & inexpensive searchable source technique in encrypted wed data," Trans. Concepts in Computer, volume. 4, number. 3, pp. 437-443, October 2016.

A modern cryptography method called searchable encryption makes it possible to browse through history. An innovative method for customer infrastructure 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 attribute table. We suggest unreliable and inaccurate that is accomplished using the asset of a stochastic trapdoor. 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. The scope of the transportation sector's coverage is always expanding.

III. EXISTING SYSTEM

Relational and analytical inquiries are crucial for blockchain applications in logistics division, e-finances, & other areas. As a result, the present blockchain system's query functionality is incredibly constrained, making it challenging to match the demands of real-world transaction applications.

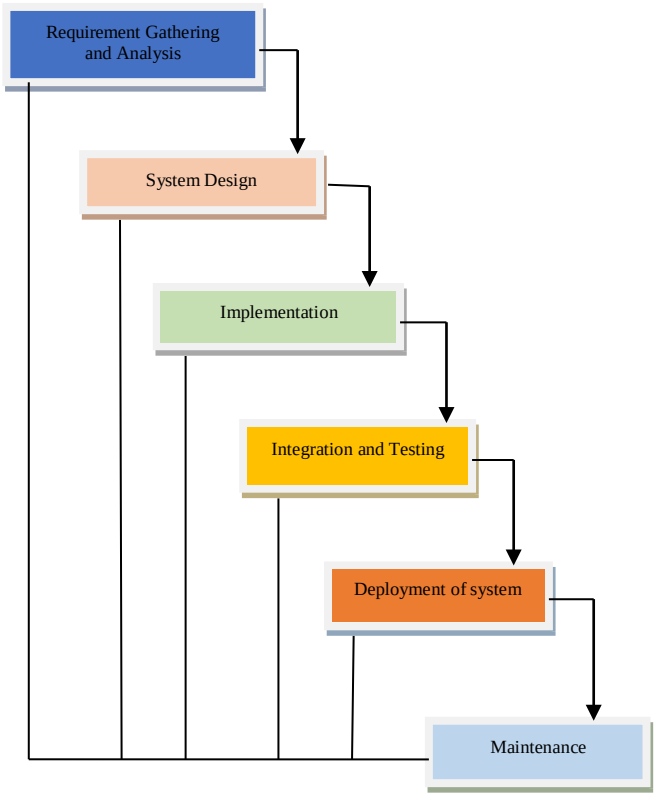
- The blockchain might lag when the network is overloadedwith users.
- Information is immutable therefore no changes can be made to it.
- Because of the way they function, blockchains are ineffective.
- The consensus process makes scaling difficult.

IV. PROPOSED SYSTEM

The suggested method encrypts sensitive information usinga symmetric encryption technique 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 is protected by the blockchain because of its decentralization and tamper-proof capabilities. The computation required for encryption and decryption is significantly decreased by this method, thus increasing the effectiveness of the suggested approach. Everyone connected to the network may access the digital record. In the distributed ledger, it is impossible to alter data. Blockchain makes it possible to trace the different data stagesand preserve the history of the data. The data cannot be altered thanks to the hash algorithm.

We adopt the waterfall model for our project's phase of software development due to its step-by-step project execution.

- ✓ **Requirement Gathering and analysis** − All prospective system requirements are gathered and compiled into a feature statement of work.
- ✓ **System Design** − The system architecture as a whole is defined as a result of this system design, which also aids in determining the system and hardware necessities.
- ✓ **Implementation** − The system is initially built as discrete detailed steps as units, which are then combined in the following phase, using insights from the systems
- ✓ integration. Unit testing consists of developing and evaluating each section for performance.
- ✓ **Integration and Testing** − Following the evaluation of every component created during the project execution, the entire system is merged. The whole system has been examined for errors and failures after integration.
- ✓ **Deployment of system** − Once the product has undergone both functional and non-functional verification, it is either published to the trade or deployed in the consumer's infrastructure.
- ✓ **Maintenance** − Many problems might arise on the client side. Tweaks are published to address certain problems. Moreover, various improved versions of the product have been launched. To bring about such modifications in the surroundings of the consumer, inspections are carried out.



V. System Architecture

The below diagram represents the workflow of the project where the uploader uploads the information about the products which are available to him/her. The uploaded information is then sent to the server as data files. But the data files that are uploaded to the cloud server get easily tampered with. So, the data files are forwarded to the blockchain where the data files are separated and stored in blocks that are interlinked with chains. Here, each block is given a unique hash functionwhich keeps the data files safe and secured from unauthorized people. The people who are having the access to the website only can able to view the data which is available on the cloud server.

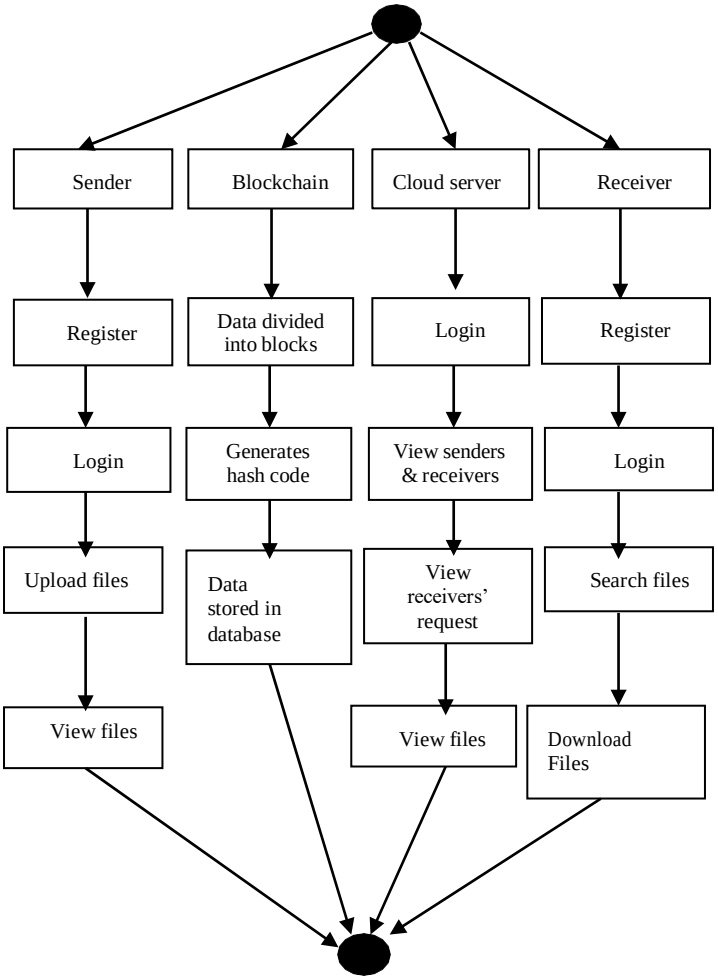


Fig 2: Block Diagram

VI. Methodology

Four components make up the proposed system: a transmitter, a receiver, a cloud server, and a blockchain. Figure 2 depicts how each component of the new methodology interactswith one another.

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. If a file is found, they can request to see it in the cloud. If the cloud accepts the request, the receiver will receive an email with the decryption key to open the file.

Cloud Server: The server will log into 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.

Blockchain: The files supplied by the sender will be separated into numerous blocks by the blockchain, each of which will be created into a hash code before being recorded in the database.

Sender: Senders must first register with their information beforethey may log in using it. They can upload their data to the blockchain once they have logged in. After the files are uploaded, the blockchain will execute the block division and hash values creation processes and store the information in a database. The sender can access their files after storing data in the database.

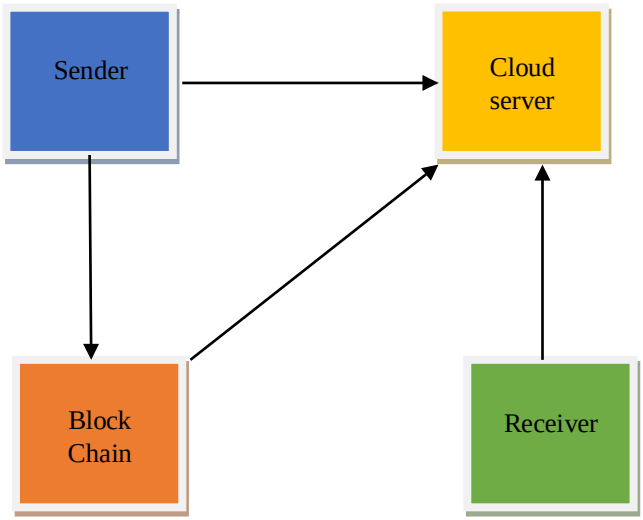


Fig 3: Component Diagram

VII. RESULTS AND DISCUSSION

Ultimately, we created a website where the sender can upload the files. The files that are uploaded to the website are divided into multiple data blocks stored in the cloud server. The receiver who wants to check the information whichis present in the files should have to get access only after getting the private key from the sender.

File id	Sender name	File name	File uploaded date	Action
1	Venkatesh	Cloud data	18-11-2022	Request
2	Ravi	Abstract for CS	20-11-2022	Request
3	Jayanth	AES	21-11-2022	Request
4	Ganesh	First file	23-11-2022	Request
5	Varun	Schooling	25-11-2022	Request

Table 1: Senders' activity

In the above table, we can see the senders count and their namesin the database. It also includes the name of the files and the uploaded date of the files are also mentioned in the table. Here, the Action column is for the receivers who want access to the file that is uploaded to the website and can able to get access from senders after sending the request to see the data in the filesthat are uploaded to the website.

File id	File Name	Hash 1	Hash 2	Date
1	Cloud Data	ab647c7b93b89	e2c55e5450715	18-11-2022
2	Abstract For CS	ab647c7b93b89	e2c55e5450715	20-11-2022
3	AES	ab647c7b93b89	e2c55e5450715	21-11-2022
4	First file	ab647c7b93b89	e2c55e5450715	23-11-2022
5	Schooling	ab647c7b93b89	e2c55e5450715	25-11-2022

Table 2: Hash code is generated for the uploaded files

The above table represents the generated hash function forthe uploaded files in the cloud server by the senders.

File id	Name	File name	Email	Private key	Status
1	Suresh	Cloud data	suresh1@gamil.com	7ccdfbbc	Accepted
2	Ramesh	Abstract for CS	ramesh23@gamil.com	5f91243b	Accepted
3	Imran	AES	imran5@gamil.com	5999a898	Accepted
4	Swami	First file	swami342@gamil.com	3b54074b	Accepted
5	Teja	Schooling	teja45@gmail.com	07e0b923	Accepted

Table 3: Receivers' Activity

The above table represents the names of the receivers and the name of the file and it also includes their email id. This table alsoshows the private key through which the data can be seen by the receivers and shows the status of the request

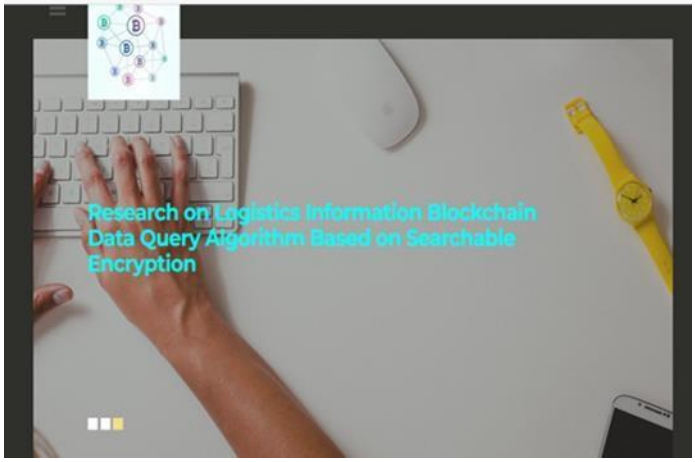


Fig 4: Home page

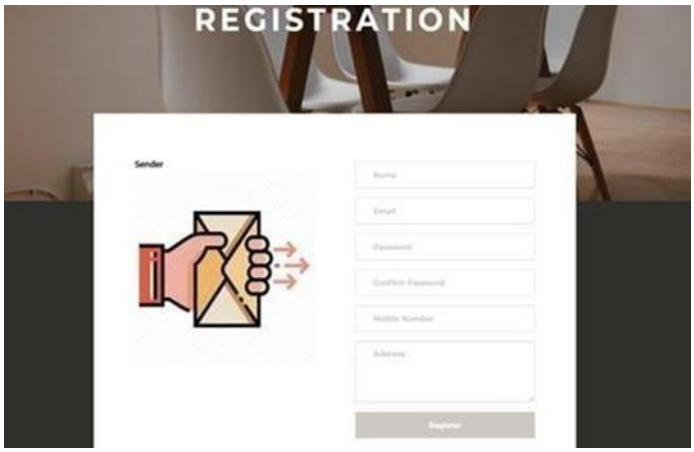


Fig 5: Senders' registration page

Senders can sign up by providing their information.

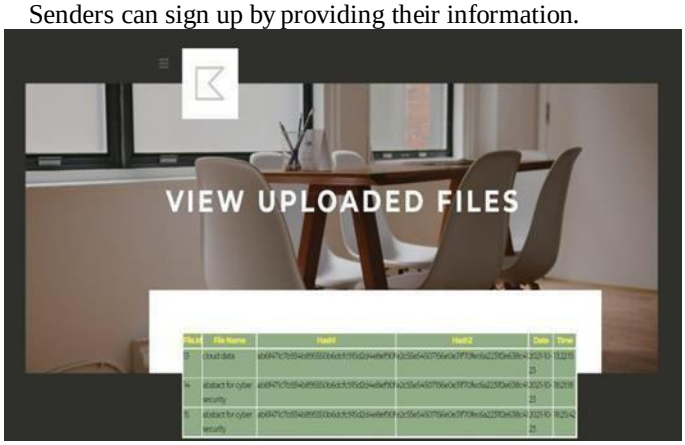


Fig 6: Generation of the Hash Function

When the sender uploads the data file to the website the datafile is converted into multiple hash functions which are highly impossible to have tampered with.

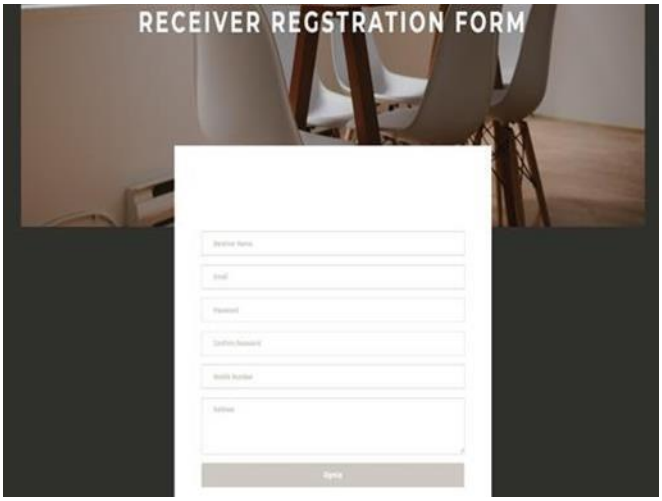


Fig 7: Receivers' registration page

Receivers can sign up by providing their information.

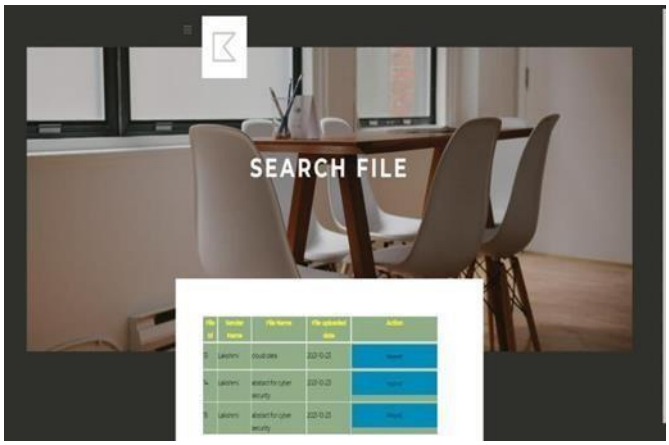


Fig 8: Download files

Here the receiver can request the required files to download from the server.

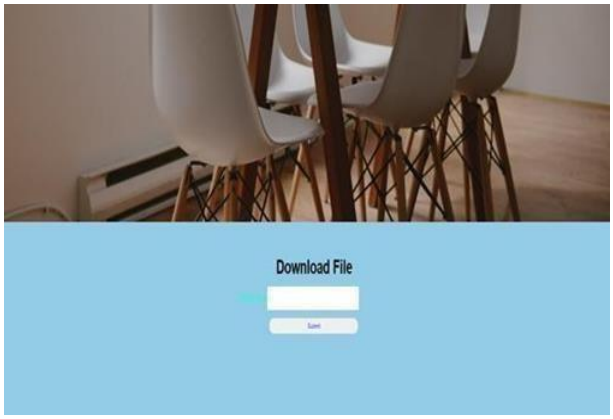


Fig 9: Download the file using the private key

Here the receiver gets access to download thefile only by getting the private key from the sender's side.

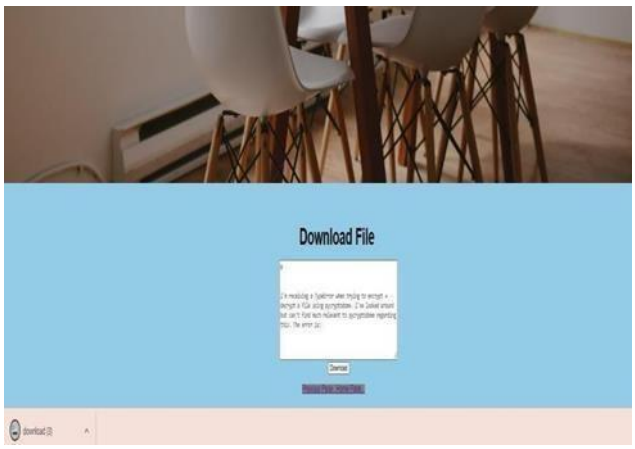


Fig 10: Downloaded file

The data in the file can be seen by the receivers in the downloaded section.

VIII. Project Outcome

As a result, by using blockchain technology in this project we can able to provide maximum security to filesthat are uploaded by the senders to the servers.

IX. Conclusion and future scope

Because there is a constant need for logistical information, a shipping data methodology based on encryption is presented to ensure data accuracy and safety by fusing benefits and employing algorithms to encrypt information. A list is created for each data set and used to search for the related data once the algorithm has encrypted information and saved it in the cloud server. The processes of data insertion and information query, as well as encryption and decryption, are all carefully designed in this study.

X. References

[1] L. Zhang, Z. Y. Zheng, and Y. Yuan, "A controlled sharing paradigm for electronic medical records based on blockchain," J. Automation., volume. 4, pp. 1–14, November 2020.

[2] Kaluza, B.; Winkler, H. Management and Controlling of Supply Chains. Int. J. Appl. Econ. Econom. IJAEE 2005, 13, 247–262.

[3] S. F. Guo, K. Liu, X. Chengi, "Electronic health records information transport strategy relying on cryptography algorithms through blockchain," Journal of Communications, vol. 43, no. 2, 2020, pp. 207–219.

[4] Tseng, M.-L., Islam, M.S., Karia, N., Fauzi, F.A., Afrin, S.: A literature review on green supply chain

management: trends and future challenges. Resources Conserv. Recycle. 141, 145–162 (2019).
[5] Q. LI and L. G. CH, "Blockchain information safety technique based on encryption," Computer. Technology., volume. 33, no. 5, pp. 147–152, 2017.
[6] Abdelhamid, M.; Hassan, G. Blockchain and Smart Contracts; ACM: New York, NY, USA, 2019; pp. 91–95.
[7] H. Qian, Li, Zhao, "Technique for transmission line interaction statistics based on blockchain technology," in Proc. 14th Intelligence Computer Technology, October 2018, pp. 326-333.
[8] Choi, T.-M., & Luo, S. (2019). Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes. Transportation Research Part E: Logistics and Transportation volume, 131, pg 139–152.
[9] J. Du, L. Liu, S. Wang, and X. Yao, "Multi-keyword navigable and evidence verifiable feature encryption system for cloud storage," IEEE Access, edition. 7, pp. 655–667, 2019.
[10] Rahardja, U.; Hidayanto, A.N.; Hariguna, T.; Aini, Q. Design framework on tertiary education system in Indonesia using blockchain technology. In Proceedings of the 2019 7th International Conference on Cyber and IT Service Management (CITSM),