EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Secured and Sustainable Supply Chain Management Using Key Escrow Encryption Technique in Blockchain Mechanism

A. Anitha [1,*], M. Priya [2], M. K. Nallakaruppan [3], Deepa Natesan [4], C. N. Kushagra Jaiswal [5] and Harsh Kr Srivastava [6]

[1,2,3,5,6]Vellore Institute of Technology, Vellore, Tamil Nadu, India
[4] SRM Institute of Science and Technology, Kattankulathur, Chennai, 603103

Abstract

INTRODUCTION: Supply chain management is the management process of the flow of goods, and services related to financial functionalities, procurement of raw materials delivery to the final destination.
OBJECTIVES: Since the traditional supply chain process lacks data visibility, trustworthiness, and distributed ledger, the need for the blockchain mechanism to ensure the time-stamped transactions to provide a secured supply chain process has been introduced and integrated.
METHODS: The distributed nature of the blockchain helps in organizing the supply chain and engaging the customers with real, verifiable, and immutable data. Blockchain technology enables these transactions to be tracked in a very secure and transparent manner. In this paper, we, therefore, propose a framework that utilizes blockchain and key Escrow encryption systems to optimize the security of supply chains to improve services for global business survivability.
RESULTS: The comparative analysis with the existing benchmarking techniques with respect to the key size, key generation time, and key distribution time was carried out with the proposed model and found that proposed work provides better results.
CONCLUSION: This proposed system can track the authenticity of the product and details about the manufacturer of that particular product. Thus, the paper concludes the proposed work enhances data's integrity, traceability, and availability and single-point failure can be resolved or reduced using blockchain mechanism.

Keywords: Blockchain, Supply chain management, Secure, Sustainable, Key Escrow, traceability

Received on 14 September 2023, accepted on 11 December 2023, published on 18 December 2023

doi: 10.4108/eetiot.4630

*Corresponding author. Email: aanitha@vit.ac.in

1. Introduction

Information systems containing confidential business information are becoming more advanced and intricate. As the system becomes more complex, the supply chains of the system become more complicated and more globalized. Therefore, we need some secure technology by which the chain of supplies of any product cannot be tracked by anyone else except the buyer and the seller who is dealing under the legal terms and conditions. Consider the following scenario for clear understanding, suppose a person X ordered a smartphone, and the delivery guy delivered the order to person X. Person X found that the smartphone was totally different than the ordered one. Now person X wants his money back, but the delivery guy is not responsible for this. Because he is just a delivery guy, not the person who created the product. These are the problems that we faced

before Blockchain, but such problems can be avoided with Blockchain Technology. In this paper, we propose Blockchain technology, as it facilitates traceability across the supply chain this means we can trace back to what actually happened to the product at each step of the supply chain. Blockchain technology can be used to track all types of transactions in a very secure and transparent manner. Blockchain has recent advantages such as a single record policy which means there will be a single record throughout the supply chain; reduces cost since there is no requirement for multiple records across the supply chain; eliminates errors and there is less human intervention, so this means the lesser the human involved the lesser the chance of errors. In supply chain management, blockchain provides permanent record-keeping, transparency, and validation of transactions shared by multiple supply chain partners. In the blockchain, transactions are recorded in a decentralized distributed ledger, due to this anyone can verify the authenticity or status of a product being delivered.

The use of Key Escrow encryption helps in involving the secured transactions between the parties to ensure the payment was completed with the product/service delivered using the deposited tokens. Thus, the proposed model helps in securing sustainable transactions with trustworthiness using blockchain mechanisms.

The rest of the paper is articulated as follows: Section 2 deals with the related work of IoT-based supply chain systems with the existing research directions on blockchain mechanisms for supply chain management. Section 3 discusses the basics of the Key Escrow algorithm in detail. Section 4 elaborates on the proposed Escrow algorithm to overcome the listed limitations, Section 5 deals with the comparative analysis of the proposed Escrow algorithm with the existing methods, and finally, Section 6 provides the conclusion.

2. Related Works

2.1. Review of IoT-based Supply Chain

The supply chain management and logistics operations can be considerably improved with the use of Internet of Things (IoT) solutions, delivering transparency and cost-effectiveness that is only possible with the use of this cutting-edge technology. Here is how IoT functions in SCM for those who are unfamiliar. The collection of real-time data on the goods being stored and carried, inventory level and shipping status, environmental conditions in warehouses and vehicles, etc., is made possible by internet-connected devices (such as images, temperature, humidity sensors, GPS trackers, etc.). After that, the raw data is processed, saved, and analyzed on the cloud to allow for continuous end-to-end supply chain monitoring and quick response to any changes.

Satyabrata Aich et al. [1], proposed an IoT-integrated blockchain supply chain which highlighted the difference between a conventional supply chain and an IoT-based supply chain. in this article, they pointed out the problems faced by the automotive industries, retail industries, and seafood industries. With the help of IoT integrated blockchain-based supply chain system, they were able to remove the problem and make the supply chain more accurate, efficient, and trustworthy, Jinhao Xie et al. [2], proposed an IoT-based supply chain in their model they divided their model into three parts intelligent warehousing, intelligent transportation, and intelligent calculation. They used sensors in intelligent transportation and big data analysis to construct central transportation scheduling. In the intelligent method, they introduced a single point-to-point identification, and in the intelligent calculation, they introduced a big data processing algorithm. The blockchain is integrated with IOT-based smart applications as discussed by Anitha et al. [3]. Also, the use of IOT in various security and monitoring systems was discussed by Anitha et al. [4-6]. Tu et al. [7], Introduced an issue of IoT adoption in logistics and supply chain management using mixed research methods. In this paper, they used meta-interference analysis with the bridge approach to develop a consensus between qualitative and quantitative findings this research notes four key factors that affect firms' intention to adopt IoT when managing their logistics and supply chain: perceived benefits, perceived cost, trust of technology, and external pressure.

Some limitations of an IoT-based supply chain are the internal struggle between operational management and IT teams, Skills being complex – and lacking, Managing and analyzing all the data being complicated Security and privacy, and Higher costs (time and money).

2.2. Review of Blockchain-based supply chain

Blockchain technology can benefit in many ways in the supply chain as it does in many other application areas. Employing blockchain in supply chain processes provides transparent, decentralized, secure, faster, and low-cost transactions. Eliminating unnecessary third parties and covering more daily life processes in digital systems minimizes paperwork. Blockchain establishes trust among trading partners. Making more detailed data available in blockchain improves supply chain monitoring ability and safety. This reduces insurance risks. Smart contracts and automated payments are game changers. They add efficiency and remove bureaucracy, especially in insurance, and traceability. They also allow Escrowed payment by keeping money until the terms of the deal are met and agreed upon and then releasing it automatically. Blockchain technology, in fact, provides the missing infrastructure that cutting-edge technologies need. Thus, increasing focus on providing integration and cooperation with technologies such as Artificial Intelligence, Big Data Analytics, Cloud Computing, and IoT will help to realize advanced supply chain systems.

Fu L et al. [8], introduced an emergency supply chain management based on blockchain technology which consists of a resource scheduling model and a resource distribution model. Raj Y et al. [9], described the various difficulties in the supply chain i.e., reduced traceability, insecurity, etc., and proposed a blockchain-based solution to overcome those difficulties. Kim et al. [10], proposed a system for the supply chain using the blockchain mechanism. They represented their system in the form of first-order logic, and later it was converted into Ethereum-based smart contracts to provide traces of goods and increase efficiency [11-13]. Mitsuaki et al. [14], proposed a blockchain-based system to solve the supply chain management system's information asymmetry and double marginalization problems. In this, they used the homomorphic encryption method to provide the security of the user data with blockchain. Haritha et al. [15] utilized the consortium blockchain and homomorphism polynomial-based private information retrieval for the secured smart parking system.

The discussed Blockchain-based supply chain systems identified the following limitations which are the motivation for the research work.

a. Lack of ability to prove the origin and quality metrics of products transparently.
b. Custom tracking systems with poor collaboration capabilities.
c. Limited certification ability and trust issues.

3 Basics of Key Escrow Algorithm

A technique for keeping crucial cryptographic keys safe is key Escrow. Each key kept in an Escrow system is associated with the original user and then encrypted for safety. Each key is saved in relation to the user who uses it, and is then returned once queried, much like a valet or coat check. By utilizing key Escrow, enterprises may make sure that their crucial keys are protected in the event of a catastrophe, such as a security breach, lost or forgotten keys, a natural disaster, or anything else. "Escrow agents" generally seen in key Escrow systems, are entities that are capable of recovering specific encrypted communication sessions or saved files. For the Escrow agent to be able to decrypt the encrypted conversation or data, such a system requires a session key encrypted with a key known to them. These crucial Escrow systems, however, are set up under the presumption that the Escrow agent is completely trustworthy; if not, one Escrow agent is configured as numerous Escrow agents. A key Escrow system, then, consists of two groups of users: entities that hold a session key (or session key information), and entities that restore it, as shown below [16-19].

- User constituent: The user constituent provides the data encryption and decryption functions. This will save the secrete key to the Escrow component.
- Key Escrow component: The storage and the distribution of the data recovery keys are managed by the key Escrow agent.
- Data recovery: The recovery component consists of algorithms, protocols, and procedures for the conversion of the plaintext to the cipher text using the information from the agent.

Thus, the key Escrow is fully trusted, and it is applied in the blockchain system where it is used with distributed ledger to apply the concept of threshold cryptography.

4 Materials and Methods

4.1 Proposed Methodology

Blockchain helps in the supply chain system to engage customers with real, verifiable, and immutable data. Both the parties involved in the transactions should ensure/agree the product is delivered after the payment is made. This is done by the passage of the token from the sender to the delivery. The process of transactions of the keys using the Escrow algorithm is listed below and the same is depicted in Figure 1 and the working of the Escrow encryption process is illustrated in Figure 2.

Steps followed for the Escrow algorithm:

1. Choose Random Session Keys for each party involved in transactions.
2. Generate Cipher Text by Encrypting the Message
3. The sender encrypts the session key with the public keys of the receiver and key Escrow agent group.
4. Upload it to the network.
5. zero-knowledge proof is attached to the data so that (ZHA) Both cipher texts are encrypting some message.
6. Sender records the hash value of Data (c) transmitted into the supply chain network & (ZHA).
7. Get data from the blockchain and obtain hash value h(c) of Cipher Text.
8. Search Cipher text with the help of hash value.

Get Session Key by Decrypting Cipher text with the receiver's private key and get a message.

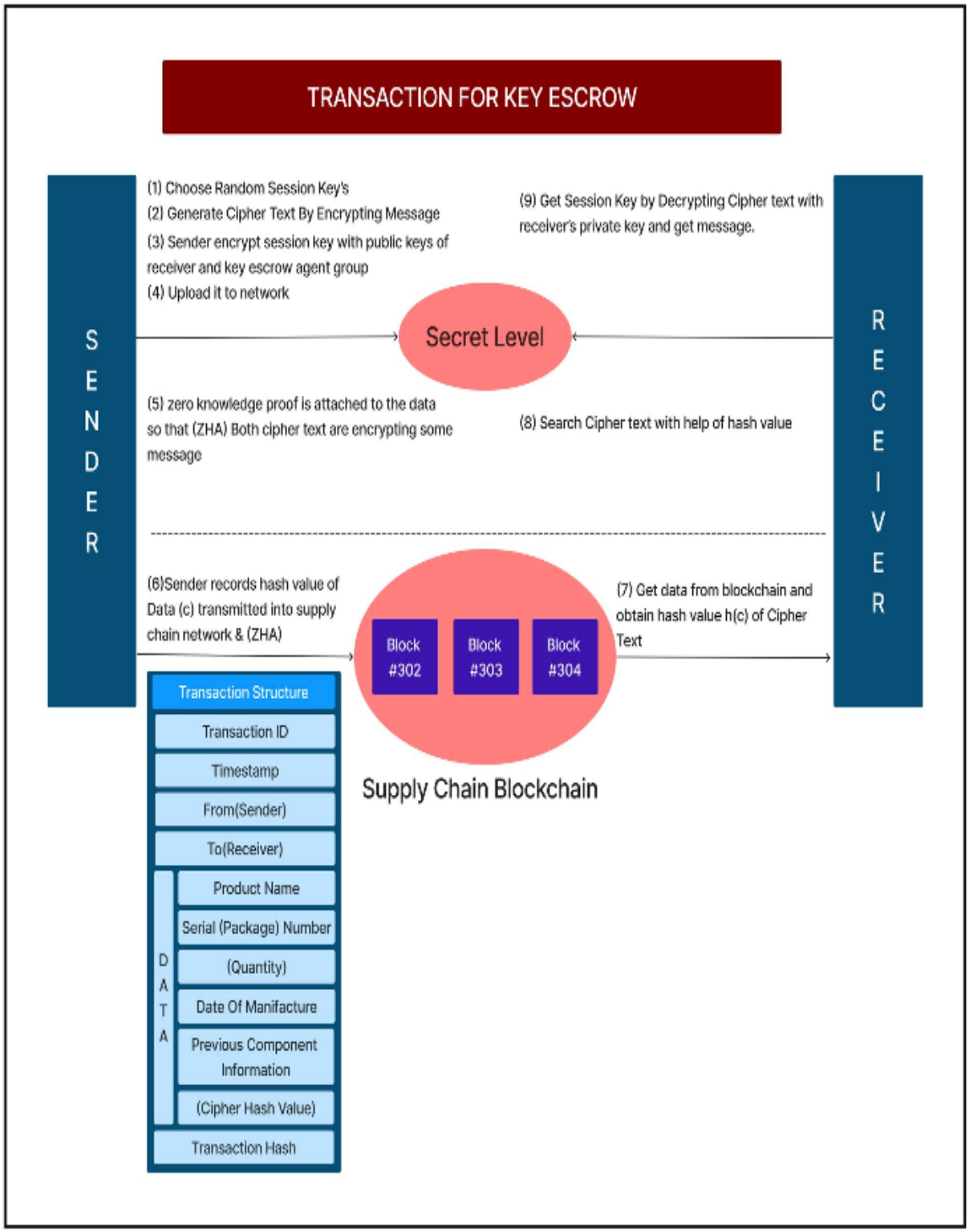

Figure 1. Proposed framework, which consists of a key Escrow network, supply chain network, and distributed storage network.

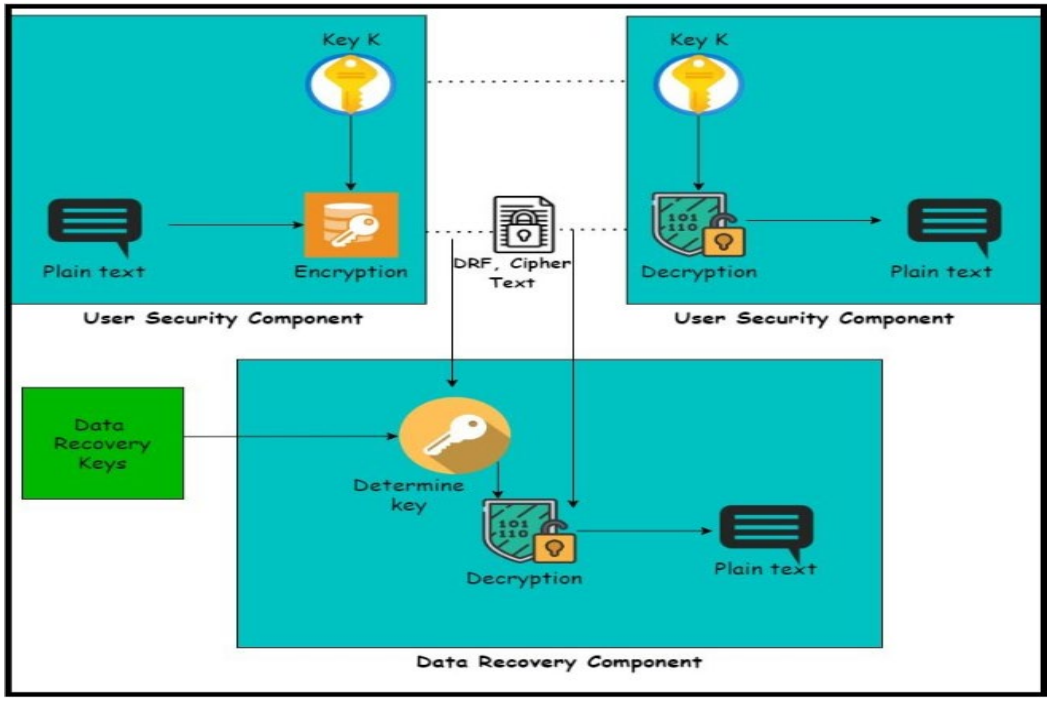

Figure 2. Working of Key Escrow Encryption Process

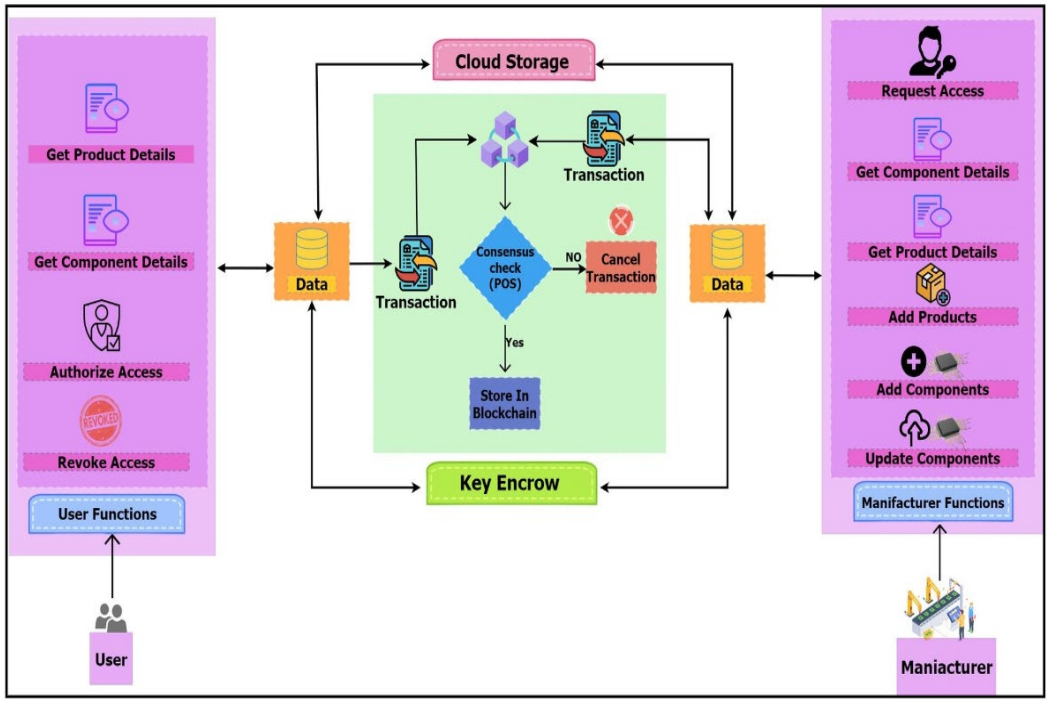

Figure 3. Proposed Architecture

4.2 Entities in the proposed system

The entities involved in the proposed supply chain system involve the buyers, manufacturer and the Key Escrow system to enhance the accessibility of the secured data and to improve the traceability with the trustworthiness as deprecated in Figure 3.

(i) Buyers: They are the owners of products, and they can check the authenticity of the product and its different components. they can check the details of the manufacturer of both products and components.

(ii) Manufacturer: they can create a product and can add it to the blockchain they can also get details about the owner of the product.

(iii) Key Escrow system: To store and manage cryptographic keys in a way that allows for their recovery in case of loss or compromise. This can be done by storing multiple copies of the key in different locations, called "Escrow," and using a mechanism for accessing the key when it is needed.

For the buyers and manufacturers, a web or mobile application can be designed so that they can easily access, store, and modify the data.

- Manufacturer app: it is a web or mobile application that can connect to any Ethereum wallet (metamask) and allows manufacturers to store, validate, and modify the products or components on the blockchain.
- Buyers' app: A web or mobile application that can be used by buyers to check the authenticity of the product and can check the manufacturer details of both products as well as different components.
- Key Escrow system: to store and manage cryptographic keys in a way that allows for their recovery in case of loss or compromise. This can be done by storing multiple copies of the key in different locations, called "Escrow," and using a mechanism for accessing the key when it is needed.

The functions of the proposed system are as follows:

- **Product Listing (Adding):** the product can be listed by the manufacturer.
  - On the blockchain. Each product is assigned a unique identification number and data about the product such as origin, manufacturing date, manufacturer address, and price of the product is captured and recorded on the blockchain.
- **Modify Products:** products that are listed by the manufacturer can be modified such as the price and description of the product.
- **Add Components:** it is possible that a product that is going to be sold may have different components that are manufactured by different manufacturers. so different components can be also added which consist of the product id in which the component will be added and the address of the manufacturer of a particular component.
- **Data Sharing and Validation:** in this study, we have used an Ethereum blockchain for validation and sharing of information. Data sharing and validation on the Ethereum blockchain is achieved through the use of smart contracts, transactions, and cryptographic techniques. Smart contracts on the Ethereum blockchain are self-executing contracts with the terms of the agreement written directly into the code. They can be used to automate the process of sharing and validating data on the Ethereum blockchain by enforcing business rules and access controls.
- **Key Escrow Encryption:** One way to use key Escrow in the blockchain is through the use of smart contracts. A smart contract is a self-executing contract with the terms of the agreement written directly into the code. In this context, a smart contract can be used to store a cryptographic key, and a predefined set of rules and conditions can be used to govern access to the key. For example, a smart contract could require multiple signatures or approvals before the key can be accessed.
- **Cloud Storage:** Cloud storage can be used to store key Escrow keys, which are used to encrypt and decrypt data in a key Escrow encryption model. By using cloud storage, it is possible to store multiple copies of the key in different locations, providing added security and accessibility. Before storing
  - The keys on the cloud storage should be encrypted and strong security measures should be taken to protect the key.
- **Workflow:** General workflow between different components/parts of the project: -
  - The manufacturer adds the product and its details on the add product function.
  - Then if buyers purchase the product, then the product manufacturer will add the address of the buyer to that product. which will make sure that this product belongs to a particular owner.
  - Components can be also added to a product if required which consists of the component name

and address of the manufacturer and product ID to which it will be added.

- If the buyer wants to check the authenticity of the product, then he/she can do it just by passing the product ID on the blockchain which will show the full information regarding that product.
- Threshold cryptography is responsible for distributing the secret key among n participants, which are key Escrow agents. The key Escrow system acts as a backup decryption system that allows authorized persons such as the government to decrypt the data when needed.
- Cloud storage provides the capability to store these distributed keys generated using threshold cryptography and encrypt them before storing them on the cloud.

Here are the steps involved in the development of a smart contract that uses key Escrow encryption.

- **Define the contract's requirements:** This step involves identifying the specific requirements for the key Escrow and supply chain management contract. This includes determining which data needs to be stored on the contract, such as the key Escrow key, product information, and supply chain data.
- **Write the contract code:** This step involves writing the code for the smart contract. This code defines the rules and logic for the contract and how it will interact with the blockchain. The contract code can be written in Solidity, a programming language specifically designed for Ethereum smart contracts.
- **Test the contract:** Before deploying the contract to the blockchain, it should be thoroughly tested to ensure that it functions as expected and that there are no bugs or errors in the code. This can be done using a local blockchain test net or using testing frameworks like Truffle.
- **Deploy the contract:** Once the contract has been tested and is ready for deployment, it can be deployed to the Ethereum blockchain. This step involves sending the contract code and a small amount of Ether (the cryptocurrency used on the Ethereum blockchain) to the blockchain to pay for the cost of executing the contract.
- **Secure the contract:** After the contract has been deployed, it's necessary to ensure that the contract and the key Escrow keys are stored and managed securely. This can be done by implementing smart contract access controls, key management software, and monitoring.
- **Monitor and maintain the contract:** After deployment, it's necessary to monitor the contract and the key Escrow keys to ensure that it's functioning correctly and that the keys are securely stored and managed. Any necessary updates or maintenance can be done by updating the contract code and deploying the updated contract to the blockchain.

The creation of the new block using the Ethereum blockchain was represented in Figure 4.

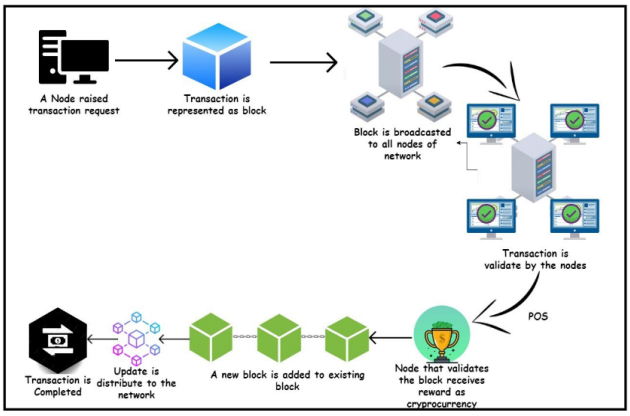

Figure 4. Creation of a new block in the Ethereum blockchain

5 Comparative Analysis

The proposed work was compared with the existing benchmarking encryption algorithms such as RSA, AES, and MPC for the key storage process. Figure 5 represents the key generation time of the Key Escrow with the RSA algorithm which is an asymmetric encryption algorithm that uses a pair of public and private keys for encryption and decryption, it is found that the number of keys generated for 160, 192 and 224 and found that proposed work works better. Similarly, Figure 6 illustrates the key storage cost for the AES where the encryption is end-to-end encryption, and the key is solely controlled by the parties who use it to encrypt and decrypt data with the proposed work with the blockchain network and found the key generation time is better with the proposed work.

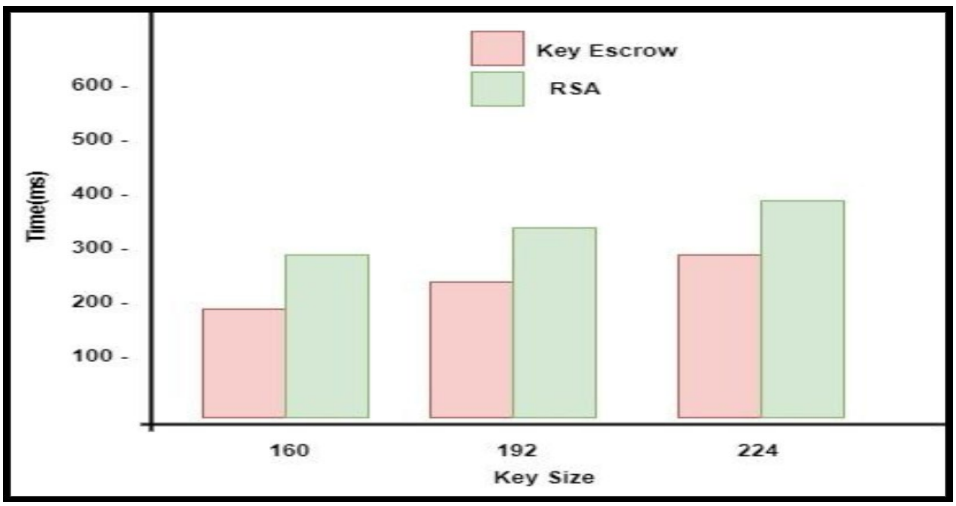

Figure5. KeyGeneration Time

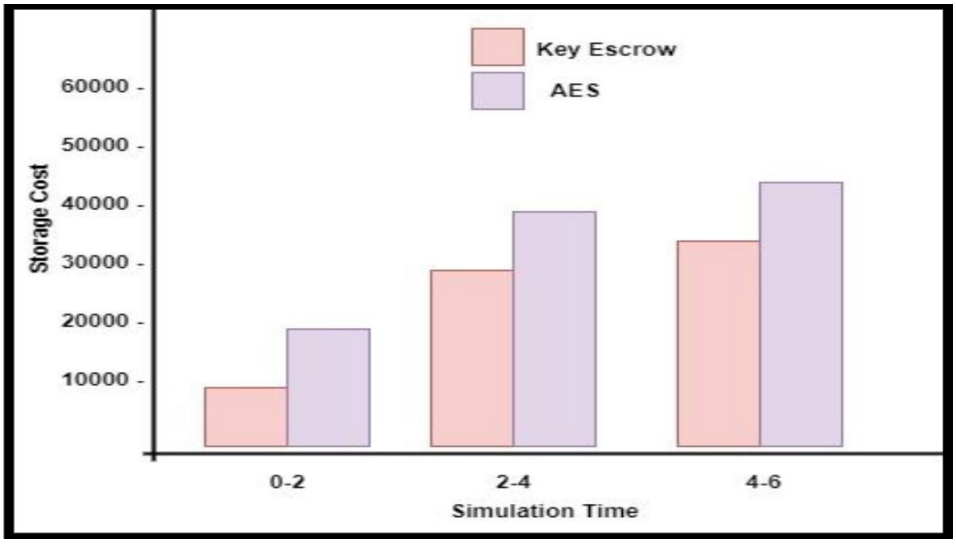

Figure 6. Key Storage Cost

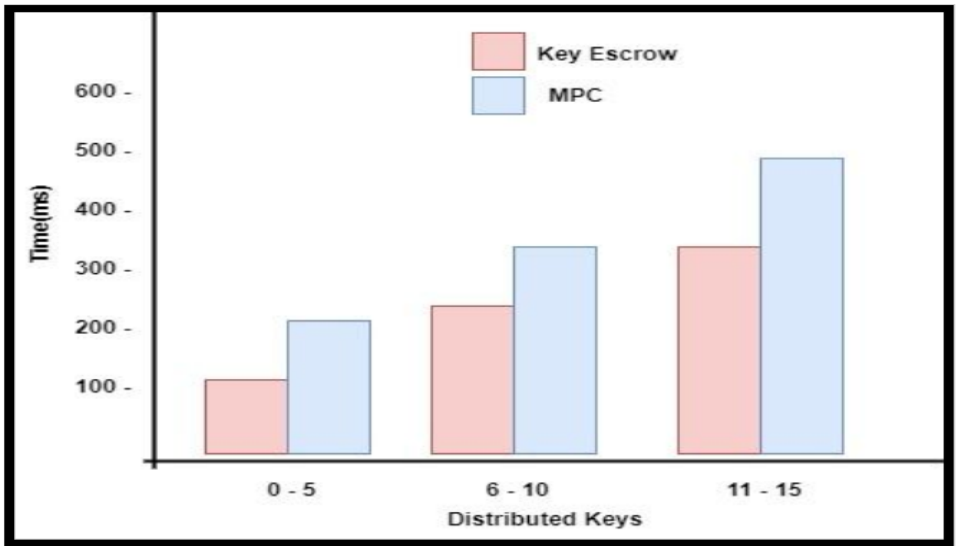

Figure 7. Key Distribution Time

6 Conclusion

In this research paper, we proposed a more secure solution for both long-lifecycle systems and small-lifecycle systems by using the integration of blockchain, cloud storage, and key Escrow encryption. This proposed system can track the authenticity of the product and details about the manufacturer of that particular product. In this paper, we also discussed how to acquire sensitive data in an unsecured or unstructured environment using key Escrow encryption. under this data's integrity, traceability, and availability are enhanced and at the same time, single-point failure can be resolved or reduced.

References

[1] Aich S, Chakraborty S, Sain M, Lee HI, Kim HC,: A review on benefits of IoT integrated blockchain-based supply chain management implementations across different sectors with case study. In2019 21st International Conference on advanced communication technology pp. 138-141(2019).

[2] Xie J, Chen C.: Supply chain and logistics optimization management for international trading enterprises using IoT-based economic logistics model. Operations Management Research. Vol. 15(3-4), pp. 711-24 (2022).

[3] Anitha, A., Haritha, T.: The Integration of Blockchain with IoT in Smart Appliances: A Systematic Review. *Blockchain Technologies for Sustainable Development in Smart Cities*, pp.223-246 (2022).

[4] Anitha, A.: Home security system using internet of things. In *IOP conference series: materials science and engineering*. Vol. 263, No. 4, pp. 042026 (2017).

[5] Anitha, A.: Garbage monitoring system using IoT. In *IOP Conference Series: Materials Science and engineering.* Vol. 263, No. 4, p. 042027 (2017).

[6] Anitha, A, Sampath N, Jerlin MA,: Smart Irrigation system using Internet of Things, International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, pp. 1-7(2020).

[7] Tu M.: An exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management: A mixed research approach. The International Journal of Logistics Management. Vol. 12;29 (1) pp. 131-51(2018).

[8] Fu L, Su JL,: Research on Technical Innovation of Emergency Supply Chain Management Based on Blockchain Technology. In2021 International Conference on Electronic Information Engineering and Computer Science (EIECS), pp. 567-571 (2021).

[9] Raj Y, Sowmiya B.: Study on Supply Chain Management using Blockchain Technology. In2021 6th International Conference on Inventive Computation Technologies (ICICT), pp. 1243-1247 (2021).

[10] Kim HM, Laskowski M,: Toward an ontology-driven blockchain design for supply-chain provenance. Intelligent Systems in Accounting, Finance and Management. (1) pp.18-27 (2018).

[11] Priya M, Kumar CA,: A novel approach for merging ontologies using formal concept analysis. International Journal of Cloud Computing.9(2-3), pp.189-206 (2020).

[12] Priya M, Ch AK,: A novel method for merging academic social network ontologies using formal concept analysis and hybrid semantic similarity measure. Library Hi Tech. 11.38(2), pp.399-419 (2020).

[13] Priya M, Aswani Kumar C.: An approach to merge domain ontologies using granular computing. Granular Computing. 6(1),pp.69-94 (2021).

[14] Nakasumi M,: Information sharing for supply chain management based on block chain technology. In2017 IEEE 19th conference on business informatics (CBI) ,Vol. 1, pp. 140-149 (2017).

[15] Haritha, T, Anitha, A.: Asymmetric Consortium Blockchain and Homomorphically Polynomial-Based PIR for Secured Smart Parking Systems. *Computers, Materials & Continua*, *75*(2), pp. 3923 - 3939 (2023).

[16] Denning DE, Branstad DK,: A taxonomy for key Escrow encryption systems. Communications of the ACM. 1, 39(3),pp.34-40 (1996).

[17] Kala MK, Priya M.: A Comprehensive Survey on the IoT-Based Electronic Healthcare Records Security, Privacy Issues, and Countermeasures Using Blockchain Technology. In2023 International Conference on Innovations in Engineering and Technology (ICIET), 13, pp. 1-8 (2023).

[18] Shirley JJ, Priya M,: A Comprehensive Survey on Ensemble Machine Learning Approaches for Detection of Intrusion in IoT Networks. In2023 International Conference on Innovations in Engineering and Technology (ICIET), pp. 1-10 (2023).

[19] T. Haritha and A. Anitha, "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System," in IEEE Access, vol. 11, pp. 114322-114340, 2023, doi: 10.1109/ACCESS.2023.3324740.