

Enriching Security at Seaport Logistics Data using Blockchain

Shital Thakar¹ and Dr. Sunil Sangve²

¹⁻²JSPM'S Rajarshi Shahu College of Engineering, Pune-411033, Maharashtra, India
Email: thakarshital@gmail.com, sunilsangve@jspmrscoe.edu.in

Abstract—The maritime industry is essential to international commerce, and significant efforts have been made over the past few decades to make it as easily accessible and unrestricted as possible. This has allowed for economic growth and global trade to continue to grow. However, the same elements that have benefited socioeconomic development from maritime commerce also make it an appealing target for terrorist groups. Bulk products and container ships equally face a variety of dangers. One of the possible flaws is structural inadequacies in the portability of cargo and watercraft. Other severe problems include document falsification and unlawful support of terrorist groups. The risks are quite high since a significant interruption to the sea transportation system may have a catastrophic impact on the world economy. Because of this, it is necessary to assess the safety and confidentiality of the goods being delivered by ship. Arguably the most efficient method for ensuring tamper-free cargo transfers across ships is the blockchain paradigm. With the introduction of the Interplanetary File System at the consignor, the blockchain formation at the cargo truck operator, and ultimately the terminal key verification when the cargo arrives at the consignee's location, this research allows efficient block initialization at the ships end. In the next portions of this study, the strategy is further evaluated, and the results are corroborated.

Index Terms— Consignor Consignee terminal key authentication, Blockchain Formation, Interplanetary File System, Seaport Management.

I. INTRODUCTION

Its maritime industry is changing quickly to satisfy the demands of multinational transportation businesses. electronically connected and functionally efficient ports are essential to fulfill increased demand and the accompanying restrictions, such as growing transportation capabilities, environmental rules, and global competition. When determining whether terminals for shipping are capable of meeting the expanding demands of handling capability, it's essential to take into consideration cost-effectiveness, technological in nature and physical infrastructure such as secondary interaction and equipment, physical location, beyond coastline transportation facilities with the value as vehicle and railroad, and safeguarded information and interaction devices, for example, maritime business structure, secondary system applications. In the framework of growth that is equitable, it is also crucial to look at the seaport's immediate surroundings.

The global trade and commerce depend heavily on the shipping sector, which is one of its most vital and crucial elements. Large countries' economies rely on the efficient movement of goods around the globe, and this sector of the economy constitutes one of the major drivers of global trade. There are several shipping lines and firms

that move goods and other bulk necessities across seas and to other nations. The precious resources that are carried on board are called cargo, and they must travel a long distance to get there—first via the shipment, subsequently to the consignee. The whole procedure opens up the possibility of malevolent behavior that might harm the cargo.

Processing of commodities within the port Despite the significance of ports to economic and social development, transportation and geographical distribution may have substantial ecological repercussions. For instance, ports might reduce traffic jams and use more ecologically friendly logistics vehicles to reduce their impact on global warming. If this extension is to be successful, there must be collaboration on both ends. First, by using newer and more efficient interior means of transport or links, product dispersion from the port's local surrounds may be enhanced with less ecological impact. Second, updating the machinery with ICTs that increase equipment dependability and effectiveness in the goods and services industries.

Dongjun Na et al. [1] consider the oracle problem along with information safeguarding, i.e., existing issues when using distributed ledger, to ensure the reliability of Dashcam video data. The V2V connection's cars are grouped together based on their GPS locations to handle the oracle problem, and a consumer is then selected to upload the transaction to the blockchain. A scenario is captured with many images, and the client compiles and publishes the action to the blockchain. Additionally, due to the permission function, only the consumer who provided any portion of the combined transaction that included confidential data initially may see the pictures. To ensure that the proposed architecture's latency has no detrimental effects on efficiency, the suggested system's overall efficiency is specifically assessed.

Jinglan Yang et al. [2] investigate the advancement of blockchain operations in the WoS repository via a combination of scientific visualisation and quantitative assessment. They use Cite Space and the VOSviewer programme. By outlining the comparative co-citation summary, lexical binding course, and co-word strategy, academics have investigated the hotspot issues and potential future research tracks in blockchain and revealed the fundamental components of blockchain development. Researchers selected significant articles, investigators, and commentaries in the area as well as recurrent themes in blockchain investigation work in order to address the main study aim. Considering these results, it is clear that the development of blockchain technology has expanded beyond the domain of cryptocurrencies, financial transaction systems, handling, and arbitration to encompass all of transactions, management, and the industries associated to these.

According to Saurabh Singh et al. in [3], the blockchain method is having an impact on the IT industry. Blockchain technology enables collaboration across organisations, groups, and even whole countries. Distributed ledger technology has attracted a lot of interest and praise because of its open architecture and peer-to-peer capabilities. The contributors of this systematic study put a lot of effort into analysing various attacks on blockchain technology and potential blockchain attacks, supporting their conclusions with pertinent empirical data. This study also looked at the many aspects of the cybersecurity challenges, impediments, flaws, and attacks that prevent the mainstream use of the technology known as distributed ledgers. The authors also described further applications and benefits of blockchain, as well as other business opportunities.

II. RELATED WORKS

Shiyuan Xu et al. [4] propose a blockchain-based method to ease the management of networked electric automobiles. Researchers utilise decentralised and EVSP, respectively, for handling enrollment and fee requests. Researchers may hide the identity of our users and the places where they are situated by employing K-anonymity, ringed endorsements, and minimal verification. Using the blockchain consensus method, transparency in provisioning resources and systematic validation can additionally be accomplished. You no longer need to depend on an EVSP or other outside company thanks to this platform. Our tests and research demonstrate that the proposed technique offers more secrecy, validity, and privacy than current approaches.

Gyeongsik Yang et al. [5] provide thorough analyses of various strategies for deploying BaaS over the cloud. The lack of analysis of infrastructure usage, the inclusion of a small number of customisable parameters, and the assessment of a very narrow spectrum of problems are only a few of the serious flaws in current BaaS research. In attempt to get beyond these limitations, researchers tested various combinations of organised elements, group measurements, package measurements, and flawed endpoints. As far as we know, agreement strategies haven't been thoroughly researched. Based on the results of the experiments, theoretical underpinnings are given for the resource degradation of the different agreement techniques, the impact of memory size and the creation of blocks rate on throughput, and the existence of two types of ordering endpoints in terms of CPU units.

In light of the development of Internet of Things devices, Zia Ullah et al. [6] highlight why concerns such information retention management, availability of information, information integrity, and data anonymity are

growing increasingly crucial. Data saved in traditional methods may become unavailable as a result of events like natural catastrophes, terrorism, or state persecution. As a result, an entirely novel data approach to the Internet of Things (IoT) has been developed that centres on the use of blockchain technology that academics have been promoting. The authors refer to this concept as the "IoT Chain Model". Authorised parties may have huge access to the data that IoT devices gather and store. It offers numerous advantages over a centralised approach, such as cheaper costs and more efficiency. IoT data distribution and storage issues are looked at.

A TDCB-D3P architecture, which combines the decentralised agreement technique with DRL, is presented by Yunyeong Goh et al. [7] in order to enhance the bandwidth and reliability results of ledgers that are distributed IoT connections. The TD-PBFT blockchain collaboration method was developed to boost stability and better defend against fraud attacks. To decide which blockchain nodes may be trusted in contributing to the agreement, the method employs a trustworthiness methodology. By analysing performance indicators and setting limitations, the proposed resolution technique takes into consideration the blockchain paradox's characteristics, such as latency, decentralisation, and confidentiality. The administrator of TDCB-DRL D3P considers the state of the dynamic blockchain architecture at the moment and selects the optimal strategies to maximise TPS while abiding by limitations.

Cloud technology is crucial for addressing the requirements of latency-sensitive technologies, such as augmented and virtual realities, and significant industrial activities, according to Gang Liu et al. [8]. Cloud servers are comparable to other network resources in terms of their geo-distributed, uncontrolled, and autonomous nature. The traditional methods of managing networks and bandwidth distribution, which often assume that possibly the necessary finances are hidden beneath a central verification node, would not be well suited for pervasive computing situations. Additionally, different businesses or individuals may be in charge of different edge devices, providing the services for wildly different prices and perhaps modifying the asset allocation in real time. They propose an intelligent system to provide access to and authorization of fog resources, enabling decentralised identification and autonomous resource provisioning for specific edge devices, to address these increasing demands.

Yustus Eko Oktian et al. [9] proposed dataflow consistency control on a network system with a secure connection. Their approach is known as SIGNORA. SIGNORA made it possible for all parties involved in a transaction to instantly authenticate the accuracy of the information being processed by merging the concepts of an electronic signature ecosystem with blockchain validation. The amalgamation of information and identities was then included into the consensus method for a still more reliable consistency guarantee via blockchain validation. The experimental results show that SIGNORA can guarantee dataflow dependability under a variety of conditions including different information packet sizes with controllable delay. Numerous off-chain solutions for lowering such costs have been considered, and costs associated with adopting smart contract technologies have also been computed. Researchers also showed that endpoints' status may be improved when they continuously operate in a trustworthy manner, but it can also be negatively impacted when they cease providing to the network. This capability of the confidence strategy was shown to be able to gather information from endpoints' prior activities.

The output of May Alhajri et al. [10] When consumers choose to disclose their fitness data to others, a variety of privacy concerns come up. This study seeks to address these problems by addressing a prominent criticism of fitness monitor data protection laws: the lack of user control over the usage of personal fitness information. Researchers created an adaptive agreement technique based on blockchain to address privacy issues. The established framework's primary outputs are the established system, requirements collecting, and formalised validation model. Additionally, the provided artefacts and the suggested blockchain implications are evaluated using the SeMF tool. The SeMF evaluation therefore confirms that the system fulfils all of its planned functions. Researchers believe the recommended approach is a smart choice for safeguarding individual privacy since it allows individuals greater control over how their medical data is utilised.

Mubashar Iqbal et al. [11] claim that cybersecurity threat administration provides a framework for analysing Sybil and Dual risks in distributed computing systems and putting their countermeasures in place. This paper presents a technique for examining the Sybil and Double vulnerabilities in open blockchains, which is based on a theoretical framework for cybersecurity threat monitoring. The methodology shows the protected or to purchases, the security risk categorizations that a hacker might take advantage of through a Network assaults the identification of barriers that end up resulting in double expenditure, the weaknesses of the threat landscape preservation and and the measures of mitigation accessible for dealing with such assaults. A recent architectural design was evaluated, and Sybil and double-spending flaws in Ethereum-based healthcare dApps were looked at as a part of the review. Additionally, writers talk on the value of distributed ledgers as well as the growing confidentiality as well as technical problems with public blockchains.

Traditional confidentiality SE systems employ cloud servers to conduct searching operations, claim Ruizhong Du et al. [12]. In order to address the problems of possibly counterfeit architecture and interpersonal attacks, this study uses blockchain techniques to establish a decentralised security paradigm. Unlike existing verification methods, the PPSE does not need the DO to confirm the results or to submit them to a private body. Directly maintaining documents in the blockchain produces reliable and immutable knowledge. As a component of an offshoring scheduling, the secret documents are transmitted to the public blockchain while the encrypted criteria remain stored in the permissioned blockchain. A permission process is also used to increase both the velocity at which inquiries can be answered and the security of the data they can hold. The results of the prototype's testing demonstrate its viability, and the safety investigation demonstrates that this strategy is somewhat secure.

III. PROPOSED METHODOLOGY

The methodology suggested for facilitating efficient security measures for seaport logistics data is depicted in the diagram displayed in Figure 1. The subsequent section outlines the steps taken to execute this strategy.

Step 1: Cargo for shipment from the Consignee – The initialization of the system occurs via the enrollment of the administrator, who supplies pertinent information in conjunction with a username and password that will subsequently be employed to obtain entry into the application's interface. Upon the administrator's successful login, the system proceeds to enroll the consignor by capturing essential information and creating a unique username and password, which will grant them the ability to access the entire system.

A user interface with interactive features has been developed to manage seaport logistics data. Frequently, seaport logistics data is vulnerable to misuse and exploitation for illicit shipments. Thus, an interactive application is being developed utilizing the swings framework within the Java programming language for this particular objective. I have gathered and uploaded the seaport logistics data pertaining to the relevant cargo at a port onto the database for safekeeping.

The consignor ships the cargo with the ultimate goal of it being delivered to the consignee by means of a series of intermediary steps. Upon dispatching the cargo, the accompanying document comprising diverse specifics of the cargo is furnished as input to the application, which subsequently assimilates the information in conjunction with the present date and time. The aforementioned particulars are transmitted to the MD5 cryptographic hash function with the intention of generating a cryptographic key. The MD5 encoding technique produces a 32-character hash value, and then a random selection of 8 characters is made. The primary key, also known as the head key, along with the relevant documents, are dispatched to the consignor who subsequently executes the subsequent stages of this procedure.

Step 2: Consignor Receiving the Cargo – The consignor is provided with both the cargo and accompanying documentation, in addition to the prior derived hash key from the system's database, including the date and time of receipt. The consignor may obtain accessibility to the hash key by signing into the system utilizing the login information furnished by the administrator. The consignor verifies the authenticity and integrity of the hash key by regenerating it using the relevant paperwork and the date and time supplied by the administrator. The aforementioned key is found to be closely associated with the hash key that is obtained by the administrator for the purpose of detecting any potential signs of an avalanche effect.

In the event that the hash key provided by the administrator and the hash key produced by the consignor are not congruent, it can be inferred that the data in transition has been subjected to a particular degree of unauthorized manipulation. In this manner, the efficacy of the sea port logistics documentation and the transported goods is upheld. After verifying the integrity, the consignor will obtain the hash key of the administrator, along with the relevant documents and the present timestamp, and utilize the MD5 the hashing process algorithm to generate a hash key and form a blockchain. The resulting key will consist of 32 characters. Eight characters will be randomly chosen from this key and, together with the hash key, documents, date, and time, will be presented to the cargo truck operator to serve as the consignor terminal key via an interactive user interface. Algorithm 1 illustrates the process of creating a blockchain.

ALGORITHM 1: Blockchain Formation

//Input : Document and Data and Time D_{DT}

//Output: Terminal Key T_{KEY}

blockchainFormation(D_{DT})

1: Start

2: $P_K = "$ " [Previous Key]

```

3: for i=0 to size of  $D_{DT}$ 
4:    $T_{PL} = B_{L[i]}$  [ $T_P$  = Database Tuple]
5:    $P_{KEY} = \text{getBodyKey}(T_{PL})$ 
6:    $T_{KEY} = P_{KEY}$ 
7: end for
8: return  $T_{KEY}$ 
9: Stop

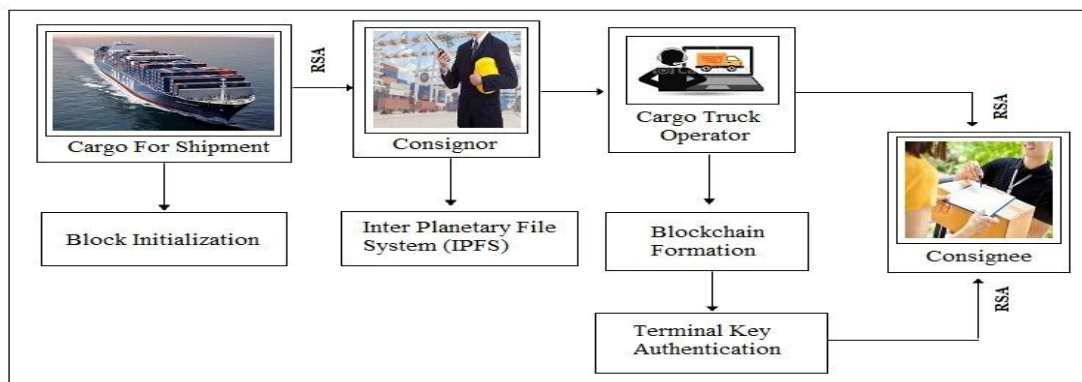
```

Step 3: Cargo Truck Operator Receiving the Cargo – The consignor will create the login ID and password for the chemist, which will be transmitted to the approved cargo truck operator to enable system accessibility. Upon obtaining system authorization, the cargo truck operator is provided with the consignor terminal key and accompanying documentation, including the present date and time, which can be used by the consignor for creating the hash key. The validation of the consignor terminal key by the cargo truck operator involves the utilization of the document, as well as the current date and time provided by the consignor as input, for the intent of evaluation. The presence of an Avalanche effect in the data suggests that it may have been subject to tampering and therefore cannot be deemed valid.

Conversely, in the event that the hash key produced corresponds with the consignor terminal key transmitted by the distributor, it can be inferred that the integrity was successfully upheld. Subsequently, the cargo truck operator shall employ the aforementioned document in conjunction alongside the consignor terminal key and the present date and time to furnish it to the MD5 hashing algorithm, thereby yielding a hash key for the cargo truck operator. Subsequently, the consignee is furnished with the Hash key, pertinent documentation, and the present date and time by the cargo truck operator. Prior to the transfer of data, it is securely protected through the utilization of RSA public key encryption. Ensuring the security of data is of utmost importance, particularly given the widespread use and high level of security associated with the RSA cryptographic algorithmic structure.

Step 3: Consignee Receiving the Cargo – The cargo truck operator generates account information for the Consignee, comprising a username and password, to enable approved entry over the system. Upon receipt of the cargo, the consignee is provided with the accompanying documentation, the cargo truck operator terminal key, and a timestamp indicating the current date and time by the cargo truck operator. The assessment of cargo truck operator terminal key integrity, obtained from the operator, is conducted by the consignee. This is done by comparing the hash formed by the data supplied by the operator.

The congruence of the hash key along with the terminal key indicates the preservation of information as well as its integrity during the entire transit process from the consignor to the consignee, who has taken possession of the cargo. In the event of a failed integrity examination and the presence of an avalanche effect, it could be inferred that the data has undergone some form of tampering or alteration. The responsible party for such actions is identifiable all the way to the cargo truck driver, given that all prior integrity checks had yielded favorable outcomes. By implementing this approach, the maintenance of the seaport logistics data's integrity is correctly ensured, as well as the dependability and authenticity of the cargo delivered to the Consignee.



IV. RESULTS AND DISCUSSIONS

The programming language Java was employed in tandem with the NetBeans Integrated Development Environment (IDE) to realize a concept for a system that facilitates the safeguarding of seaport logistics data

through the utilization of a blockchain implementation. The system in use employed a laptop that was furnished with an Intel i5 processor, 8 GB of Random Access Memory (RAM), and 1 Terabyte (TB) of storage capacity on its hard drive. The MySQL database server has proficiently fulfilled its responsibilities pertaining to database management and storage capabilities.

The study examined the productivity of the seaport logistics data approach that utilizes RSA encryption and blockchain. This was achieved through the implementation of a series of rigorous experiments. The subsequent segment expounds upon the results of the evaluation and the criteria utilized for evaluation.

The feasibility of the suggested approach has been thoroughly evaluated. The following section presents the empirical results of the experimental investigation.

Encryption and Decryption Time performance

The proposed methodology employs encryption and decryption methodologies to ensure the privacy of seaport logistics data during transmission to various stakeholders involved in the implementation process. By adhering to the procedures delineated in this section, an individual can assess the efficacy of this methodology. Table 1 presents a comprehensive analysis of the time required for encryption and decryption of data employing the RSA method, based on the growing amount of characters in each turn. The data is displayed in a tabular form as illustrated in Table I.

TABLE I. ENCRYPTION AND DECRYPTION TIME PERFORMANCE

Number of Characters	Encryption Time (in ms)	Decryption Time (in ms)
16	4	4
1809	16	18
2809	34	33
3013	47	55
5004	53	57
5790	65	63
6343	68	65
8427	78	79
9211	83	82
9992	97	98

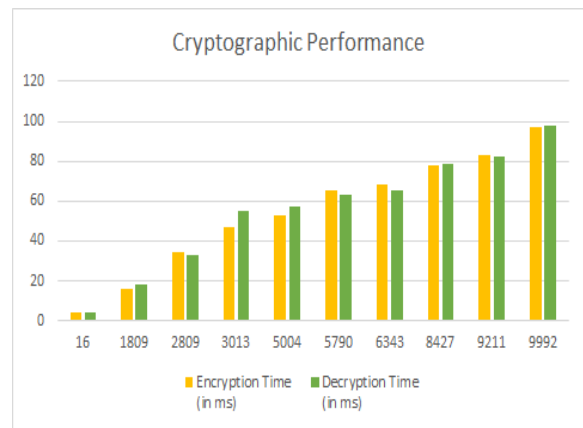


Figure 2: Encryption and Decryption Time

The graphical illustration depicted in Figure 3, in the form of a bar chart, is appropriate for facilitating a visual analysis of the data presented in Table 1. It is evident that there is no direct correlation between the length of the input and the time required for encryption and decryption processes. The rationale behind this is that the RSA encryption method employed in this approach has been extensively researched and effectively applied in this methodology. The experimental findings indicate that the approach is being executed in a reasonably satisfactory manner.

Throughput Analysis of Blockchain Transaction

The present study assesses the efficacy of utilizing blockchain technology to safeguard seaport logistics data, specifically in terms of the throughput of blockchain transactions. To attain this objective, an experiment is conducted wherein a set of seaport logistics data is utilized to generate the blockchain multiple times. Upon the addition of a novel logistics data file, the blockchain undergoes an update. Subsequently, the frequency of blockchain transactions is computed on a per-second basis. Table 2 presents the calculated outcomes, while Figure 3 displays an appropriate plot.

The obtained outcome is compared with the discoveries presented in reference [13], wherein blockchain technology was employed to scrutinize the throughput on Hyperledger fabric. The methodology employed in the creation of the blockchain involved the utilization of multiple seaport logistic files to facilitate transactions on the blockchain implementation. The transactions utilized in [13] exhibit a level of comparability to the transactions employed in our deployment, resulting in equivalent computational expenses during the execution of blockchain transactions

Table II. Blockchain Transaction Time Estimation Table

S no.	Number of Seaport Logistics Files	Blockchain Transaction Rate	Throughput
1	100	11123	111.23
2	200	12364	123.64
3	300	14889	148.89
4	400	16897	168.97
5	500	17646	176.46

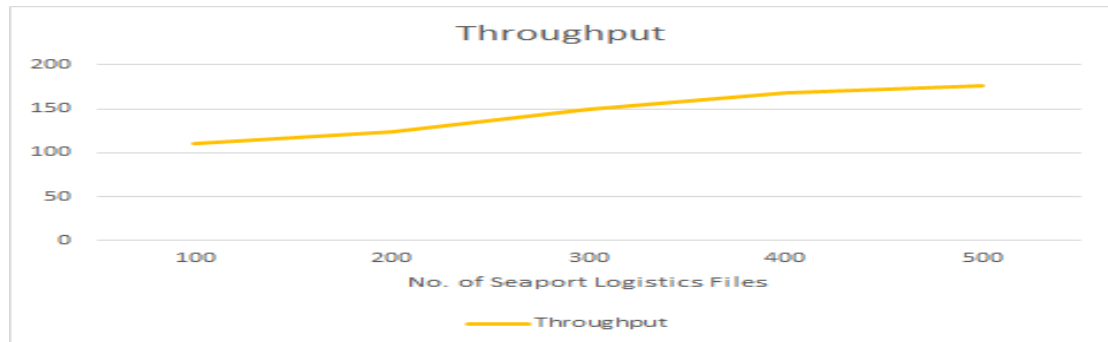


Figure 3: Transaction per Second

TABLE III. COMPARISON OF BLOCKCHAIN TRANSACTION PERFORMANCE

Methodology	Throughput (in tps)
Our Approach	145.83
Hyperledger Fabric based approach in [13]	128.2

The study conducted in reference [13] reports an average throughput of 128.20. According to the data presented in Table 2, the suggested approach yields a AVERAGE throughput of approximately 145.83. Table 3 presents a comparison of the various approaches, while Figure 4 provides a visual representation of the same. The utilization of the RSA cryptographic methodology facilitates an efficient realization that upholds the integrity of the blockchain. This factor constitutes a significant proportion of the distinction between our proposed approach and the technique outlined in reference [13], thereby establishing the superiority of our suggested model over that of [13].

V. CONCLUSION AND FUTURE SCOPE

This research outlines a proposed methodology for safeguarding seaport logistics data through the utilization of the Java programming language in a systematic and methodical manner. Cargo shipments are a highly crucial and time-sensitive aspect of transportation logistics. The utilization of seaport logistics data is instrumental in obtaining pertinent information regarding cargo and ensuring its safety and security. The transmission of shipment particulars to the multiple stakeholders involved in this situation can potentially result in security breaches or interference. Consequently, the logistics data of the seaport is transmitted to the MD5 hashing algorithm with the aim of generating a key. The MD5 cryptographic hash function produces a 32-character hash value, from which a random selection of 8 characters is made. The key and accompanying logistics documents are dispatched to the consignor. The individual responsible for sending the shipment confirms their access to the system profile and validates the key. They then package the hash key of the truck operator, alongside the relevant documentation and the current timestamp, and submit it to the MD5 hashing algorithm to generate a hash key and establish a blockchain. This information is subsequently transmitted to the recipient of the shipment. Upon accessing the system, the consignor proceeds to authenticate both the key and the blockchain's integrity. Subsequently, a new blockchain transaction is generated through key generation and transmitted to the

cargo truck operator. Upon receipt of the documents, the consignee will perform a conclusive assessment of the blockchain's integrity, thereby validating the dependability of the seaport logistics methodology. The potential for future expansion of this research concept includes real-time execution and development as an app for smartphones to enhance operational ease.

REFERENCES

- [1] D. Na and S. Park, "Blockchain-Based Dashcam Video Management Method for Data Sharing and Integrity in V2V Network," in *IEEE Access*, vol. 10, pp. 3307-3319, 2022, doi: 10.1109/ACCESS.2022.3140419.
- [2] J. Yang, C. Ma, D. Li and J. Liu, "Mapping the Knowledge on Blockchain Technology in the Field of Business and Management: A Bibliometric Analysis," in *IEEE Access*, vol. 10, pp. 60585-60596, 2022, doi: 10.1109/ACCESS.2022.3179714.
- [3] S. Singh, A. S. M. S. Hosen and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," in *IEEE Access*, vol. 9, pp. 13938-13959, 2021, doi: 10.1109/ACCESS.2021.3051602.
- [4] M. D. Firoozjaei, A. Ghorbani, H. Kim and J. Song, "EVChain: A Blockchain-based Credit Sharing in Electric Vehicles Charging," 2019 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 2019, pp. 1-5, doi: 10.1109/PST47121.2019.8949026.
- [5] G. Yang, K. Lee, K. Lee, Y. Yoo, H. Lee and C. Yoo, "Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric," in *IEEE Access*, vol. 10, pp. 74902-74920, 2022, doi: 10.1109/ACCESS.2022.3190979.
- [6] N. Wang et al., "Secure and Distributed IoT Data Storage in Clouds Based on Secret Sharing and Collaborative Blockchain," in *IEEE/ACM Transactions on Networking*, 2022, doi: 10.1109/TNET.2022.3218933.
- [7] Y. Goh, J. Yun, D. Jung and J. -M. Chung, "Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning," in *IEEE Access*, vol. 10, pp. 118498-118511, 2022, doi: 10.1109/ACCESS.2022.3220852.
- [8] G. Liu, J. Wu and T. Wang, "Blockchain-enabled fog resource access and granting," in *Intelligent and Converged Networks*, vol. 2, no. 2, pp. 108-114, June 2021, doi: 10.23919/ICN.2021.0009.
- [9] Y. E. Oktian, S. Heo and H. Kim, "SIGNORA: A Blockchain-Based Framework for Dataflow Integrity Provisioning in an Untrusted Data Pipeline," in *IEEE Access*, vol. 10, pp. 89714-89731, 2022, doi: 10.1109/ACCESS.2022.3199878.
- [10] M. Alhajri, C. Rudolph and A. S. Shahraki, "A Blockchain-Based Consent Mechanism for Access to Fitness Data in the Healthcare Context," in *IEEE Access*, vol. 10, pp. 22960-22979, 2022, doi: 10.1109/ACCESS.2022.3154106.
- [11] M. Iqbal and R. Matulevičius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems," in *IEEE Access*, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.
- [12] R. Du, C. Ma and M. Li, "Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains," in *Tsinghua Science and Technology*, vol. 28, no. 1, pp. 13-26, February 2023, doi: 10.26599/TST.2021.9010070.
- [13] M. Kuzlu, M. Pipattanasomporn, L. Gurses and S. Rahman, "Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 536-540, doi: 10.1109/Blockchain.2019.00003.