Grenze International Journal of Engineering and Technology, June Issue

A Comprehensive Review on Securing Seaport Logistics Data using Blockchain

Shital Thakar[1] and Dr. Sunil Sangve[2]
[1-2]JSPM'S Rajarshi Shahu College of Engineering, Pune-411033, Maharashtra, India
Email: thakarshital@gmail.com, sunilsangve@jspmrscoe.edu.in

***Abstract*—The shipping industry is one of the most essential as well as one of the critical components for the trade and commerce of the entire world. This industry is one of the biggest contributors for international commerce and economies of large nations are dependent upon the smooth flow of cargo and shipment across the world. There are extensive shipping lines and shipping companies that transport cargo and other bulk essentials through the oceans and across to different countries. The cargo in the ships is a valuable resource and is subjected to extensive travel its destination, which goes through the shipment and then all the way to the consignee. This entire process can allow for some kind of malicious activity that can be detrimental to the cargo. Therefore, there is a need for the evaluation of the security and privacy of the cargo that is being shipped through the shipment. The paradigm of blockchain is one of the most effective mechanisms that can be utilized for the tamper free transfer of the cargo through ships. This research enables effective block initialization at the ships end with implementation of Interplanetary File System at the consignor and the blockchain formation at the end at the cargo truck operator and finally the terminal key authentication when the cargo reaches the destination at the consignee. The approach is further elaborated in the next version of this research.**

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

I. INTRODUCTION

To meet the needs of international shipping companies, the seaport business is undergoing fast change. In order to meet this consumption and the associated constraints, such as increasing transportation capacities, ecological regulations, and international rivalry, digitally-enabled and operationally-efficient harbors are crucial. Affordability, technological and physical facilities which include peripheral connectivity and apparatus, physical region, away from the coast transportation facilities such as truck and rail, and protected content and interaction devices for instance, maritime organization framework, peripheral system software are all important factors to take into account when ensuring that shipping ports can meet the growing needs for processing capacity. It is also important to examine the nearby areas of the seaport in this paradigm of balanced expansion.
Commodities processing at the port's interior Transport and regional transmission may have significant ecological effects, despite the importance of ports to commercial and social growth. For instance, ports could lessen their contribution to global warming by minimizing gridlock and switching to environmentally efficient logistical trucks. There must be cooperation on both ends if this expansion is to succeed. First, from either the

Grenze ID: 01.GIJET.9.2.533

port's immediate surroundings, by taking use of newer and more effective interior transportation services or linkages, products dispersion may be improved with less ecological influence. Second, according to port's perspective, modernizing the equipment with ICTs that boost reliability and productivity in the good and services business.

Maritime sector is crucial to international commerce, and enormous steps have indeed been undertaken in last several decades to make it as accessible and unhindered as feasible, so facilitating even further expansion of global trade and the economy. Yet, the same factors that have made marine shipping a boon to socioeconomic growth also make it an easy target for terrorist organizations. Container ships and bulk commodities both face a wide range of threats. Structural compromises in the stability of cargo and boats are only one of several potential weaknesses. Documentation forgery and illegal funding for terrorist organizations are two other serious issues. Last but not least, the consequences are extraordinarily high since a major disruption in the marine transportation network could have a devastating effect on the global economy.

Under this context, authorities have implemented measures to close one of most glaring attack vectors in the marine transport system. Although majority of these steps were still being adopted at the moment of typing, this paper attempts to estimate their expense at this preliminary phase. However, this survey did reveal three major findings. The first concern is that doing nothing might wind up costing a lot of money. Terrorists may attempt to attack or take advantage of the marine transportation sector. If the assault is huge and well, administrations may be forced to shut off the whole system while they try to implement countermeasures. These could either be extreme, like the shutdown of port facilities, or ineffective, like long, unnecessary cargo inspections at both the sender and recipient terminals.

The argument is that the expense of not doing anything is likely to be far higher than the cost of taking action, even if certain expenses are easier to estimate than many others. It is not hard to estimate how much it will charge to build a ship given that it requires just a few capital investments of specialized tools and a small amount of labor at standard, well-established prices around the globe. Consequently, a responsibility must be accomplished in order to provide unbreakable security for the products in transit from consignor to consignee.

According to Ruizhong Du et al. [1], conventional confidentiality SE systems use cloud servers to carry out searching activities. This research utilizes blockchain solutions to provide a decentralized security paradigm to counteract the issues of potentially fraudulent infrastructure and individual assaults. The PPSE eliminates the need for the DO to validate or to submit the findings to a private entity, unlike current verification techniques. Keeping records in the blockchain directly yields trustworthy and unchangeable information. The encrypted criterion is kept in the permissioned blockchain, whereas the encrypted records are sent to the public blockchain as part of an offshoring arrangement; additionally, an authorization mechanism is implemented to bolster both the speed with which queries can be processed and the safety of the data they contain. The safety study shows that somehow this approach is secure, and the prototype's test findings prove that it can be put into practice.

To assure the trustworthiness of Dashcam video data, Dongjun Na et al. [2] take into account the oracle issue and data protection, i.e., current problems when employing distributed ledger. To address the oracle issue, the vehicles in the V2V connection are divided into groups according to their GPS coordinates, and then a consumer is chosen to send the operation to the blockchain. Multiple picture data for a scene are recorded, and the client gathers and uploads the activity to the blockchain. Also, the customer who originally sent any part of the consolidated transaction that contains sensitive information is the only one who can see the photographs thanks to the authorization feature. In particular, the recommended system's total throughput is evaluated to make sure that the suggested architecture's latency does not negatively impact efficiency.

The work of May Alhajri et al. [3] There are a number of privacy issues that arise when people decide to share their fitness information with others. This research aspires to solve these issues by giving users more say over how personal fitness information is used, which is a common complaint about fitness monitors' data protection laws. To help with privacy concerns, we developed a blockchain-based adaptive agreement method. The developed system, requirement gathering, and formalized verification model are the main deliverables of the developed framework. In addition, the SeMF instrument is used to assess the presented artefacts and the indicated blockchain implications. Thus, the SeMF assessment verifies that the system accomplishes all of its intended purposes. Since the suggested method gives users more say in how their fitness data is used, researchers think it is a good option for protecting individual privacy.

The second part of this paper is devoted to an analysis of the existing literature as the related works, the third part describes our proposed methodology, and the fourth part finishes with suggestions for future study and research recommendations.

II. Related Work

In [4], Saurabh Singh et al. describe how the blockchain approach is influencing the IT sector. Businesses, communities, and even nations may all work together using blockchain technology. Because of its distributed ledger and peer-to-peer functionality, distributed ledger technology has gained widespread attention and admiration. The authors of this systematic review have done extensive work analyzing many assaults on block chain technology and the possible attacks of blockchain, illustrating their findings with relevant empirical evidences. In addition, this article explored the many facets of the cybersecurity difficulties, obstacles, weaknesses, and assaults that thwart widespread implementation of distributed ledger technology. Additional uses and advantages of blockchain were also outlined by the writers, and other prospects for businesses were highlighted.

Zia Ullah et al. [5] explain why issues like information storage administration, accessibility of information, integrity of information, and data confidentiality are becoming more important in the face of the proliferation of Internet of Things devices. Due to factors like natural disasters, terrorism, or governmental repression, data stored using conventional ways may become inaccessible. The outcome is a new information strategy for the Internet of Things (IoT) based on the blockchain technology that the academics have been pushing forward. This model is referred to as the "IoT Chain Model" by the authors. The data collected by IoT devices may be stored and accessed by authorized parties on a massive scale. The benefits it provides over a centralized system are many, including lower costs and higher efficiency. Challenges in storing and distributing IoT data are investigated.

When it comes to agreement techniques for deploying BaaS throughout the cloud, Gyeongsik Yang et al. [6] provide in-depth evaluations. Current research on BaaS has significant shortcomings, including an absence of study of infrastructure use, the incorporation of just one and more customizable factors, and the evaluation of a very small range of defects. To overcome these restrictions, researchers conducted extensive tests with different configurations of ordered components, group dimensions, package dimensions, and defective endpoints. So far as we are aware, agreement techniques just haven't been studied in such depth. Theoretical foundations on the resource depletion of the various agreement methods, the influence of memory space and block generation frequency on throughput, as well as the presence of strong and weak ordered endpoints in regards to CPU units, are provided predicated on the experimental outcomes.

According to Gang Liu et al. [7], Cloud technology is essential for meeting the needs of latency-sensitive technologies including virtual reality, augmented reality, and important manufacturing operations. When it comes to network resources, cloud servers are similar to others but stand out due to their geo-distributed, unsupervised, and standalone nature. Pervasive computing scenarios would not be well to the conventional approaches to network management and bandwidth allocation, which often presume that perhaps the adequate funds are located behind a central verification node. Furthermore, various organizations or persons may control separate edge devices, selling the services at vastly varying costs and possibly adjusting the asset availability in real time. To meet these emerging needs, we suggest an intelligent system for providing accessibility to and giving permission to use fog resources, which would allow for decentralized identification and the autonomous provisioning of resources for individual edge devices.

To improve the bandwidth and reliability outcomes of distributed ledgers IoT networking, Yunyeong Goh et al. [8] present a TDCB-D3P architecture which combines the decentralized agreement approach with DRL. To better withstand fraudulent assaults and increase stability, the TD-PBFT blockchain agreement mechanism was created. The technique uses a trustworthiness mechanism to determine which blockchain servers may be relied upon to contribute to the agreement. The suggested resolution method takes into account the blockchain paradox qualities, including delay, decentralization, and privacy, by analyzing throughput indicators and establishing limits. TDCB-DRL D3P's operator takes into account the current condition of the dynamically blockchain system and chooses the best possible measures to maximize TPS whilst adhering to restrictions.

In order to facilitate the handling of networked electric cars, Shiyuan Xu et al. [9] suggest a blockchain-based solution. When it comes to enrollment and fee processing, researchers use decentralized and EVSP, correspondingly. By using K-anonymity, ringed signatures, and negligible verification, researchers are able to conceal the identities of our users and the locations at which they are located. Accountability in resource provisioning and automated validation may also be achieved via the use of blockchain consensus mechanism. This platform eliminates the need to put your faith in an EVSP or other external service. Our testing and research prove that the suggested approach provides superior confidentiality, legitimacy, and privacy than existing methods.

Dataflow consistency management on an unsecured network system was introduced by Yustus Eko Oktian et al. [10]. Their methodology is called SIGNORA. By fusing the ideas of a signature network with blockchain confirmation, SIGNORA enabled all parties engaged in a transaction to verify the authenticity of information being processed in real time. For an even more robust consistency assurance utilizing blockchain confirmation, the combination of the information and signatures was then embedded in the consensus mechanism. The experimental findings demonstrate that SIGNORA is capable of providing dataflow reliability assurance across a wide range of information packet size situations with manageable latency. Expenses associated with using smart contract approaches also have been calculated, and numerous off-chain options discussed for reducing those expenses. In addition, researchers demonstrated that the confidence mechanism can learn from the past actions of endpoints, improving their standing whenever they demonstrate consistently trustworthy conduct and lowering everything when they stop contributing to the network.

Employing Cite Space and the VOSviewer application, Jinglan Yang et al. [11] examine the development of blockchain experiments in the WoS database via the lenses of scientific visualization and quantitative evaluation. Researchers have explored the hotspot difficulties and future study paths in blockchain, as well as disclosed the underlying elements of blockchain development by sketching the comparison co-citation outline, lexical coupling track, and co-word plan. In answering the primary research objective, researchers identified major publications, scientists, and editorials in the field, in addition to recurring topics in blockchain investigative work. In light of these findings, it is evident that blockchain technological progress has moved beyond the realm of cryptocurrencies, monetary transactions systems, handling, and resolution to include all of commerce, administration, and the sectors related to these.

According to Mubashar Iqbal et al. [12], cybersecurity threat administration offers a framework to study Sybil as well as Double threats in distributed infrastructure and implement their solutions. This study introduces a methodology for investigating Sybil as well as Double vulnerabilities in public blockchains, which is predicated upon that cybersecurity threat monitoring conceptual framework. The methodology depicts the guarded or to investments, the security risk classifications an intruder could exploit via a Network attacks, the recognition of challenges that result in dual expenditure, the shortcomings of threat landscape, and the mitigation strategies available to deal with those attacks. Sybil and double-spending vulnerabilities in Ethereum-based medical dApps were investigated as part of an evaluation of a recently developed architecture. Additionally, authors discuss the rising privacy and operational problems of public blockchains, as well as the importance of distributed ledgers.

Information exchange has emerged to be among the IoT's foremost significant uses, according to Kwame Opuni-Boachie Obour Agyekum et al. [13]. Researchers present a protected identity-based PRE data-sharing mechanism in a cloud computing setting, ensuring the anonymity, trustworthiness, and confidentiality of shared information. The IBPRE method enables access control to protect personal their protected information on the cloud and conveniently distribute it with authorized personnel. An edge node serves as an intermediary to do the demanding calculations because of the lack of central processing power. The method additionally takes advantage of ICN capabilities to efficiently distribute preloaded material, which boosts operation performance and allows for better use of available network capacity. Then, researchers provide a concept of a blockchain-based mechanism that provides authorization on encrypted information with some wiggle room. Data providers may better protect their confidentiality with the aid of this perfect authentication mechanism.

III. Proposed Model

This article conducted extensive research into existing methods with the end goal of developing the approach shown in the flowchart below. The approach initiates with the start state where the cargo data is provided along with the cargo for shipment, this data is then utilized for the block initialization from the consignor. The interplanetary file system is being used for the purpose of achieving the data storage, the cargo truck operator also initiates the blockchain formation which results in the terminal key generation. The output is achieved as the cargo security and then reaches the stop state.

IV. Conclusions

When it comes to global trade and business, the shipping sector is a crucial cog in the wheel. The prosperity of major economies is tied to the efficiency with which goods and services are transported throughout the globe, making this sector very important. Cargo and other bulk provisions are transported across the seas by a plethora of shipping lines and shipping businesses. A ship's cargo is a precious commodity that endures a long journey to reach its final destination, from the shipper through the carrier to the consignee. At any point throughout this

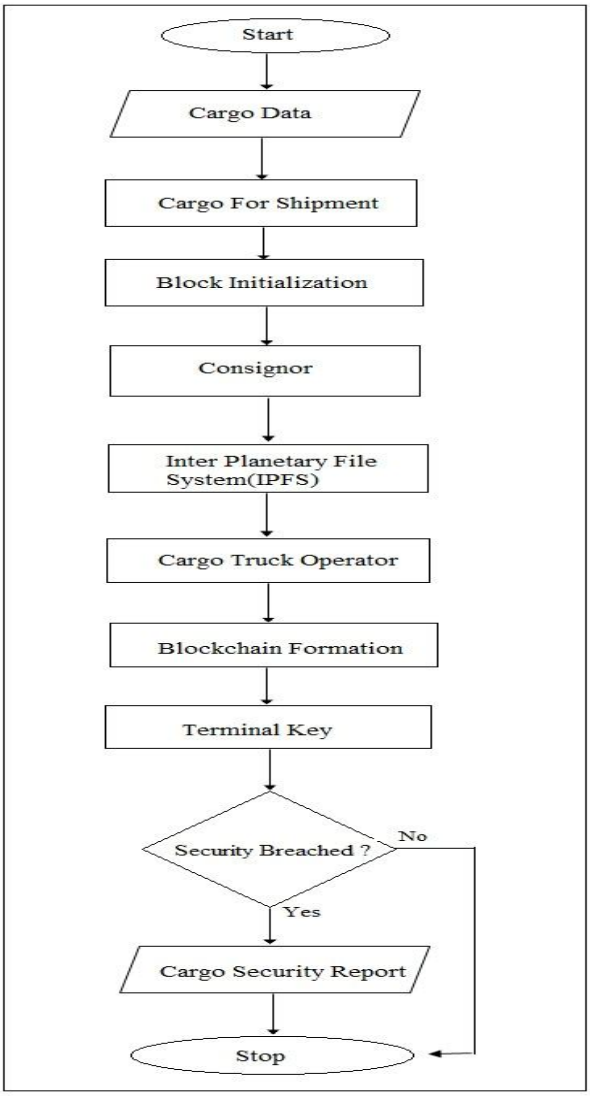

Figure 1: Proposed model

chain of events, criminals may be able to do damage to the shipment. As a result, it is important to assess the safety and confidentiality of the shipment's contents. The blockchain paradigm is one of the most powerful mechanisms that can be deployed to ensure the integrity of the transfer of goods between ships. This study paves the way for efficient block initialization at the ships' end, IFS implementation at the consignor, blockchain generation at the end at the cargo truck operator, and terminal key authentication at the end at the consignee. In the revised edition of this study, the methodology will be fleshed out in more detail.

REFERENCES

[1] H. Ahmed and M. A. Ismail, "Towards a Novel Framework for Automatic Big Data Detection," in IEEE Access, vol. 8, pp. 186304-186322, 2020, doi: 10.1109/ACCESS.2020.3030562.

[2] S. Zhou, J. He, H. Yang, D. Chen and R. Zhang, "Big Data-Driven Abnormal Behavior Detection in Healthcare Based on Association Rules," in IEEE Access, vol. 8, pp. 129002-129011, 2020, doi: 10.1109/ACCESS.2020.3009006.

[3] S. Nazir et al., "A Comprehensive Analysis of Healthcare Big Data Management, Analytics and Scientific Programming," in IEEE Access, vol. 8, pp. 95714-95733, 2020, doi: 10.1109/ACCESS.2020.2995572.

[4] Z. Hu and D. Li, "Improved heuristic job scheduling method to enhance throughput for big data analytics," in Tsinghua Science and Technology, vol. 27, no. 2, pp. 344-357, April 2022, doi: 10.26599/TST.2020.9010047.

[5] Y. Gao, X. Chen and X. Du, "A Big Data Provenance Model for Data Security Supervision Based on PROV-DM Model," in IEEE Access, vol. 8, pp. 38742-38752, 2020, doi: 10.1109/ACCESS.2020.2975820.

[6] G. Zhai, Y. Yang, H. Wang and S. Du, "Multi-attention fusion modeling for sentiment analysis of educational big data," in Big Data Mining and Analytics, vol. 3, no. 4, pp. 311-319, Dec. 2020, doi: 10.26599/BDMA.2020.9020024.
[7] M. Li, Z. Liu, X. Shi and H. Jin, "ATCS: Auto-Tuning Configurations of Big Data Frameworks Based on Generative Adversarial Nets," in IEEE Access, vol. 8, pp. 50485-50496, 2020, doi: 10.1109/ACCESS.2020.2979812.
[8] W. Zhong, N. Yu and C. Ai, "Applying big data based deep learning system to intrusion detection," in Big Data Mining and Analytics, vol. 3, no. 3, pp. 181-195, Sept. 2020, doi: 10.26599/BDMA.2020.9020003.
[9] M. Li, H. Wang and J. Li, "Mining conditional functional dependency rules on big data," in Big Data Mining and Analytics, vol. 3, no. 1, pp. 68-84, March 2020, doi: 10.26599/BDMA.2019.9020019.
[10] G. T. Reddy et al., "Analysis of Dimensionality Reduction Techniques on Big Data," in IEEE Access, vol. 8, pp. 54776-54788, 2020, doi: 10.1109/ACCESS.2020.2980942.
[11] A. Guezzaz, Y. Asimi, M. Azrour and A. Asimi, "Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly detection," in Big Data Mining and Analytics, vol. 4, no. 1, pp. 18-24, March 2021, doi: 10.26599/BDMA.2020.9020019.
[12] X. Zhou, Y. Hu, W. Liang, J. Ma and Q. Jin, "Variational LSTM Enhanced Anomaly Detection for Industrial Big Data," in IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 3469-3477, May 2021, doi: 10.1109/TII.2020.3022432.
[13] M. Dener, S. Al and A. Orman, "STLGBM-DDS: An Efficient Data Balanced DoS Detection System for Wireless Sensor Networks on Big Data Environment," in IEEE Access, vol. 10, pp. 92931-92945, 2022, doi: 10.1109/ACCESS.2022.3202807.