International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Study on Supply Chain Management System Using Blockchain and IoT Technology

Hai-Shui Yan*, Hyung-Ho Kim, Jun-Won Yang*****

Submitted: 06/06/2022 **Accepted:** 10/09/2022

Abstract

The Internet-of-Things (IoT) expanded rapidly, resulting in many services, software products, and electrical devices integrated with sensors. It is associated with protocols that are currently under development. Blockchain technology serves as the foundation for most IoT-based applications, and it must be adaptable and widely disseminated to guarantee their survival. Blockchain-based IoT has several limitations due to its resource-constrained nature, including security, scalability, traceability, efficiency, and network throughput. The suggested method in this paper is a Privacy-assisted Information Exchange Framework (P-IEF), an integrated security mechanism that detects suspicious activities in sensor nodes and locates them on a blacklist. This approach is a centered digital ledger procedure that ensures the privacy of all nodes and ensures that the data can be validated without modifying any node, and there is no need for a third party to secure data. The simulation analysis shows trust measures and open challenges, and research difficulties examined in IoT environments. The privacy-assisted information exchange framework has achieved a security ratio of 98.25 %, a scalability ratio of 97.15 %, traceability rate of 98.54%, efficiency rate of 99.01 %, and network throughput ratio of 97.19 % outperforms compared with other approaches.

Keywords: *Blockchain, Internet of Things, Security, Privacy-assisted information exchange framework*

[1]1. Introduction

The adoption of the internet of things has expanded. In the future, many objects will be linked together through the internet of things (IoT), enabling M2M communication between machines (humans and machines). Furthermore, it's becoming more difficult to function without access to the Internet of Things (IoT). Many of the gadgets we use daily are both networked and linked to the internet [1]. Recently, the number of smart gadgets, wireless sensors, and related technologies has increased dramatically. Still, they are just a few of the limitless domains in which it might be implemented, enabling an unlimited number of applications [2]. Developing and deploying IoT effectively needs secure data transmission between devices and maintaining the privacy, availability, and integrity of shared resources and information while adhering to self-organizing behavior [3]. The likelihood of threats, dangers, and cyberattacks on connected devices will escalate as the number of devices rises. As a result of weak security, entities lead to victims of cyberattacks and other types of attackers, such as malware [4].

Internet of Things (IoT) refers to the novel stage of the internet or the growth of the internet and the World Wide, where a large number of things will be linked and permit immediate communication between machines referred to as Machine-2-Machine Communication (M2M) [5]. Most of the IoT components, hardware, and software are fundamental, but sensors operate as IoT's sensory systems and serve as the foundation for blockchain technology. As far as the Internet of Things is concerned, blockchain is its backbone in privacy concerns. Blockchain plays a critical role in developing and expanding the IoT by allowing low-end devices with limited resources, thus providing game-changing services to such devices [6]. Henceforth, it makes use of all sensors linked together wirelessly. In the future, low-

[1] * Doctor of Business Administration, CEO, Shanghai Aurora Information Technology Group Co., Ltd., China, yanhaishui@gmail.com
**Professor, Dept. of Air Transport and Logistics, Sehan University, Korea
hhkim@sehan.ac.kr
***Professor, Dept. of Air Transport and Logistics, Sehan University, Korea (Corresponding Author)
jwyang@sehan.ac.kr

cost and miniature IoT wireless sensors can be available because of advanced sensor technology, enabling intelligent home appliances of all sizes [7]. Sensor nodes having the ability to sense, communicate, and analyze data make up a typical blockchain. When used as a platform for other domains, blockchain provides an important environmental detection and characterization in supply chain management while also ensuring that communications are secure and reliable. Further, blockchain can also be used for military monitoring, medical and healthcare monitoring, various types of industry, and traffic surveillance [8].

Blockchain faces serious dangers and technological obstacles that must be solved to assure their adaption and spread. The resource constraint objects nature of blockchain is largely to blame for their shortcomings [9]. Sensors in an open space owing to blockchain's sensitivity to severe or adverse environmental conditions such as high degrees of humidity or pressure or other impurities, it is important to have sensor nodes with high levels of resilience and robustness [10]. Other issues and obstacles faced in blockchain methodology include limited resources, limited communication ability, consistency, power quality, throughput, flexibility, precision in results, dependability, confidence, transparency, diversity, connectivity, an uncertain environment, and denial of service attacks (DoS) [11]. In addition, blockchain has special concerns that have captured the interest of researchers and the previously described general difficulties they face. Blockchain's open research problems include energy usage, network longevity, bandwidth, wirelessly routing technologies, and privacy [12].

Privacy is indeed crucial in communication networks. Researchers have difficulty figuring out the most effective, safest, and least-cost means to get data packets to their destinations [13]. The researchers' blockchain is implemented due to limited energy, restricted computation, and a short communication range [14]. Since it reduces data transmission to the gateway node by aggregating data inside the member nodes and minimizing energy consumption, this information exchange framework is recognized as the energy-efficient protocol [15].

This information exchange framework divides the network into hierarchies to balance the load and fulfill additional goals like flexibility, energy minimization, and lifespan optimization [16]. Blockchain lifetime and network performance may both be extended and influenced using this method. A cluster head is selected based on critical factors such as transmission power and proximity to the sink node when using hierarchal or cluster-based routing protocols [17].

Clone leader rotates dependent on the nodes' rank. Hence, the rise and fall in the values of key parameters determine the node's rank. The cluster head aggregates data from cluster members, serves as a coordinator, and sends it to the base station or satellite node. Block clusters, grid clusters, and chain clusters are the three primary routing protocols based on their use of clusters. Blockchain-based security must also include protection against hostile nodes [18-19]. Illegal access to information disrupts and degrades several aspects of the network, including longevity, throughput, authenticity, secrecy, and integrity.

Further, to deal with the threats mentioned earlier, IoT needs a blockchain approach that is dependable, effective, and durable. As a result of these factors, this research attempted to extend network lifetime, boost throughput, raise the number of active nodes, minimize packet delay and packet loss, and energy usage while also improvising to handle hostile nodes. The following is the contributions in the P-IEF:

- Examines the current system's shortcomings, how blockchain might be used to address them, and their role in providing safety
- This method evaluates and summarises a wide variety of current consensus algorithms
- Provides an analysis of the basic concerns of scalability and interoperability is provided, along with solutions that are currently accessible

This paper is categorized as follows: In section 2, a quick summary of related research and literature. The suggested system model is detailed in section 3. In section 4, the result and discussion are reviewed and discussed. Section 5 summarizes the findings.

2. Materials and Methods

2.1 Literature Review

Hader et al. [20] presented blockchain technology in the retail market. Analysis of the effect of blockchain integration in the retail sector and a study of how organizations might use blockchain in the retail industry to promote customer loyalty and improve supply chain management. This study brings a new perspective to the previous research on supply chain performance in the retail business using blockchain technology. When it comes to supply chain enterprises or loyalty programs, blockchain technology might create secure, decentralized ledgers and smart contracts that remove the need for intermediaries, thereby leading to more efficient transactions and operations.

Yousuf et al. [21] investigated the supply chain's current difficulties and evaluated their suitability for blockchain technology deployment. To develop a generic framework, trust and decentralization were analyzed in terms of their respective qualities. They provided a conceptual framework for ongoing research and development in blockchain and supply chain management. A preliminary framework concentrates on

evaluating the applicability of blockchain in the supply chain phases of customer orders, supplier involvement, production flow management, and demand management were developed. Each level of the supply chain was studied for challenges that would necessitate trust and decentralization to qualify for blockchain deployment.

Jiang et al. [22] discussed blockchain technology's fundamental structure, operational properties, and basic categorization. As a supply chain finance expert, the authors examined how blockchain technology is used in many aspects of the supply chain finance industry. The goal is to stabilize the supply chain financial development process and encourage the robust growth of the financial sector. Supply chain finance may be made more efficient via the use of blockchain technology. The enterprise's electronic vouchers and transaction records may be traced back and have a high degree of accuracy. Fraud detection and an enhanced decision may be achieved using this method, increasing transaction security and minimizing transaction costs.

Niya et al. [23] introduced a platform-independent, generic-purpose, and blockchain-based supply chain tracking method. They have used a supply chain technology application that uses the supply chain on the Ethereum blockchain. In this decentralized application, numerous item combinations may be monitored with specific instance design and its use. Trustworthy and transparent tracking is facilitated via the public ethereum blockchain, a platform-independent, generic-purpose, and blockchain-based supply chain tracking method.

Yue et al. [24] examined and developed a blockchain-based supply chain management approach for medical equipment. The whole life cycle supply chain management model was used to build a medical equipment supply chain supervision model based on blockchain technology. As a result, a medical equipment management information system was developed that covers the complete life cycle of medical equipment from production to disposal. This allows for better oversight of procurement processes and better control over costs while ensuring the safety and quality of healthcare products and services.

Ahamed et al. [25] proposed distributed ledger that would connect farmers with consumers. The blockchain can hold data from the point of a catch to the delivery to the final customer. A vital part of delivering high-quality and safe products and avoiding monetary losses was effective temperature monitoring and the persuasive data management of temperature information. For cold supply chain management, they used blockchain technology to cut down on food waste and boost consumer confidence using this technology in the supply chain.

2.2 Analytical Methods

In the field of information technology, blockchain technology is one of the most recent developments. It is an immutable record of transactions distributed across the network participants enabling safe and trustless transactions. The term "blockchain" refers to the combination of a distributed ledger, authentications, and encryption technology. Nodes are the network members in the blockchain. Nodes may perform one or more of the following functions, depending on their role in the network; (a) begin transactions, (b) verify transactions and blocks, (c) construct blocks, and (d) retain a copy of the ledger. A basic node in the network originates transactions, but a complete node in addition to launching transactions verifies all transactions and blocks and keeps a copy of the ledger. The basic system model for privacy-assisted information exchange framework (P-IEF) is exposed in Fig.1. There are two types of blockchain networks: public and private blockchains. A user may join a public blockchain network without obtaining permission from the network administrator. According to their needs, a user may join the network as a basic, validating, or complete node. To make the network more secure, public networks generally compensate users who participate in consensus.

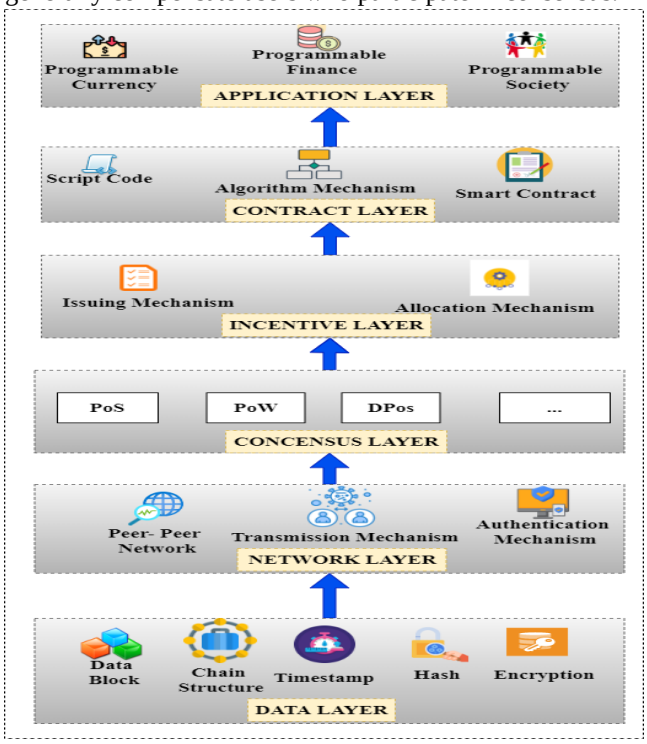

Figure. 1. Basic system model for privacy-assisted information exchange framework (P-IEF)

The open-source nature of the network means that patient privacy is at risk because of its open nature. There are scalability concerns with the public blockchain because of the open network involvement. However, a private blockchain is an open invite network that needs users' approval from an authenticating authority before joining the network. It is up to the network authority to determine the duties of network members.

Private blockchains have higher throughput. They are more scalable since there are fewer network members to validate and replicate data than public blockchains. Provenance, authenticity, property data, and anticounterfeiting are possible with blockchain, a time-stamped collection of immutable data records. Trading, provenance, and location information are hashed and connected to blockchain transactions in blockchain-based supply chains. A cryptographic hash is used to bind these transactions into blocks, making them unchangeable. Unsolicited confirmation of supply chain events is especially important in the food supply chain, where tracing items' origins or pinpointing fraud, as in the case of the horsemeat scandal or an epidemic of salmonella in papayas, is a necessity. IoT and blockchain-facilitated supply chain is mentioned in Fig. 2.

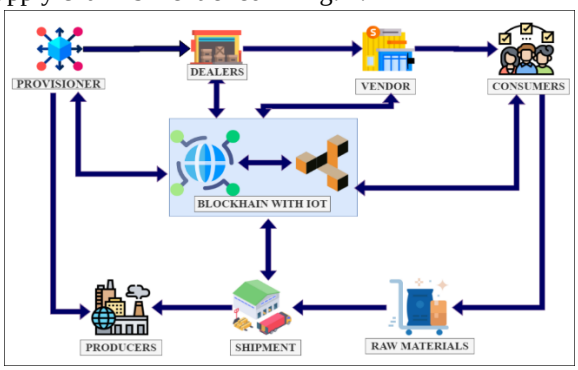

Figure 2. IoT and Blockchain-facilitated supply chain

To ensure supply chain traceability and integrity, there are two fundamental requirements: As a first step, tamper-proof records of supply chain occurrences, product properties, IoT sensor status information, and other additional data sources and regulatory endorsements must be kept in a secure location. The collected data must be genuine and symbolize accurate observations of sensor devices, events in the supply chain, and other auxiliary information. Commodities, sensor readings, supply chain occurrences, and other additional pieces of information are captured in a tamper-proof manner. The distributed tamper-proof ledger provided by blockchain technology meets the first condition. The key objective is to build trust in information at the source to guarantee that the data recorded on a blockchain is trustworthy. When it comes to building trust, it is important to evaluate the many commodity categories, the entities involved, and their relationships since supply chains are made up of many different entities and product categories. In addition, the procedure has been automated, allowing for real-time tracking and auditing of the data. As part of our proposed P-IEF framework, we offer a security and reputation mechanism that analyses the authenticity of supply chain information and provides fine reputational evaluations for goods and supply chain participants at a perceptual level.

Transactions in the data layer are carried out in this section by recording supply chain events like creating a new commodity, changing the entities such as reputation, and commodities, including the modifications of ownership on the ledger and the data layer transactions. Data layer transactions comprise the transaction creation (N_{Tr}), the transaction trading (X_{Tr}), the sensory transaction (S_{Tr}), the regulator transaction (R_{Tr}), and the commodity transaction (C_{Tr}). A primary producer issues a create transaction N_{Tr} to validate the new commodity creation and specification of the qualitative smart contract to which this new commodity will be connected in a ledger. A primary producer issues a new transaction creation attribute N_{Tr} to validate the new commodity arrival and identify the standard of the smart contract where these commodities are connected. In a standard smart contract, terms and conditions for quality evaluation, such as maximum/minimum temperature limits, rating criteria, and so on, have been agreed upon in advance.

The transaction creation is given by the Eq (1):

$$N_{Tr} = [IC|G_h|PD_l|PD_{agreement}|A_j|O_j] \quad (1)$$

where IC is the commodity's identification, G_h is its hash, PD_e is its owner's identify, and $PD_{agreement}$ is the quality agreement identifier to which the commodity is tied. The commodity owner's signature and public key are A_e and O_e, respectively. Commodities may be transferred amongst supply chain organizations as they move from the primary producer to the retail shelf. Fig 3 displays the flow diagram for creating new transactions.

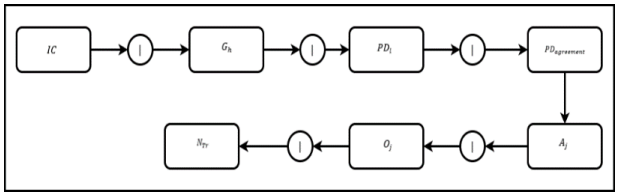

Figure 3. Flow diagram for creating new transactions

The actual transfer of a product from the seller to the buyer is confirmed by the trade transaction X_{Tr} :

$$X_{Tr} = [IC|G_h|PD_b|PD_{agreement}|A_i|O_i|A_e|O_e] \quad (2)$$

As in Eq (2), N_{Tr}'s commodity's identification (IC) and PD_l are swapped with PD_b, the buyer's unique identification. There are four types of public keyswith signatures: the vendor's signature (A_i), the consumer's signature (A_e), and the vendor's public key (O_i) and consumer's public key (O_e). Using N_{Tr}, IoT devices that monitor the temperature of a commodity and record this information on the blockchain using sensory transactions, S_{Tr}. Device IDs are used to identify gateway nodes in the IoT, and the nodes themselves produce these transactions. Decoupling the pace of this transaction from the real rate of commodity trading is

essential. Fig 4. pinpoints the path diagram for a trade transaction.

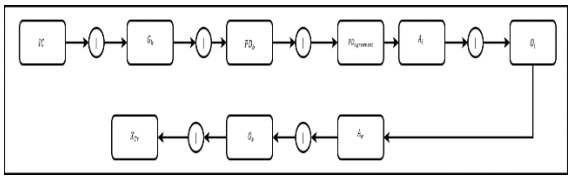

Figure. 4. Path diagram for a trade transaction

Before a trading event, the commodity is regularly inspected when items are kept in storage. Sensory transaction (S_{Tr}) is conveyed through Eq (3):

$$S_{Tr} = [IC|G_h|A_{sig}] \quad (3)$$

Where IC defines the commodity identification, G_h gives the hash value representation of information from sensors, A_{sig} denotes the gateway node's signature may be found in the IC field of the commodity. The regulator transaction (R_{Tr}) assigns a rating for the seller, $R_{REG}(y)$, after conducting a physical examination of a storage facility.

$$R_{Tr} = [PD_b|G_h|B_{com}] \quad (4)$$

Eq (4) exhibits the regulator transaction calculation. PD_b represents the identification of seller, G_h signifies the hash value for inspection evidence, B_{com} implies the commodity type for which a score is awarded. Each commodity guarantees that the regulator's rating is recorded discretely since the storage conditions and assessment bodies may change with various forms of a commodity transaction. Additionally, regulators must conduct regular inspections of the facility and offer updated ratings to verify that it meets quality and safety criteria. The frequency of these on-site inspections is low. The regulator's rating decreases whenever the site has not been investigated over an extended period of time or the regulator's evaluation is bigger than the evaluation period. Commodity transaction is produced when a retailer receives a commodity to record the completion of the supply chain on the blockchain.

$$C_{Tr} = [IC|A_g|O_g] \quad (5)$$

As highlighted in Eq (5), IC symbolizes the Commodity identification of the retailer, O_g and A_g are the public keys and the signature of the retailer who received the product, respectively. The primary goal of this transaction is to maintain track of products that have passed the product chain since products that do not have a product chain may suggest that they are counterfeit. A seller's reputation might improve or deteriorate. Thus this trust value must be adjusted accordingly. The trustworthiness of a trader may also be affected by additional application-specific variables apart from the reputation score based on buyer, commodity, and regulator ratings. The trust score of a trader is:

$$Trust_d(m_n) = \rho_0 \times V(m_n) + \rho_1 \times w_1 + \rho_1 \times w_2 + \ldots\ldots\ldots + \rho_n \times w_n \quad (6)$$

According to Eq (6), the trust score of a trader $\mathrm{Trust_d(m_n)}$ is calculated using the overall reputation $\mathrm{V(m_n)}$ and several additional feature scores $\mathrm{w_1, w_2, w_3 \ldots, w_n}$. Here, $\rho_1, \rho_2, \ldots, \rho_2$ specifies the weighting factors set by the network administrator of a corporate network.

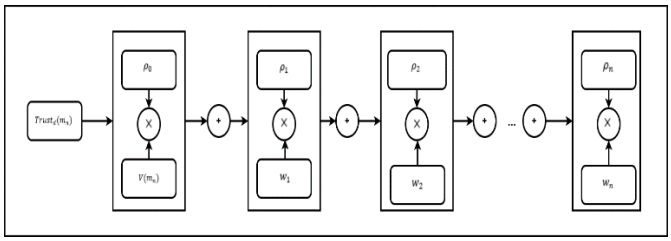

Figure 5. Flow diagram for trust score of a trader

Flow diagram for the trust score of a trader is mentioned in Fig 5. The trust and reputation module calculates trust scores and stores them in the profiles of traders. The trust and reputation module calculates trust scores and stores them in the profiles of traders. Every trader must maintain a minimum degree of trust. Whenever $\mathrm{Trust_d(m_n)} < \mathrm{Trust_d(minimum)}$, the network administrator is notified of the trust level breach through a notice message. The network administrator may withdraw the trader's participation in the network after receiving the notice.

3. Results and Discussion

Data created by IoT devices have been gathered and distributed more fairly using blockchains, allowing for decentralized data. The supply chain is a multi-faceted system that includes a wide range of participants and components. Holistic and central digital efforts have already contributed to the integration and standardization of its fragmented processes: purchasing, ordering, manufacturing, and transporting. The transaction data offered by the cooperative supply chain platform may be used to precisely assess the user's trade conduct, trade relationships, fund usage habits, and trading tactics. The transaction data offered by the cooperative supply chain platform may be used to correctly assess the user's trade behavior, trade relations, fund usage habits, and trading strategies. Additional benefits include better risk management and in-depth industry research owing to the increased availability of data. Risk control reports can be generated for management in a time-efficient manner by analyzing the risk profile of consumers. The technology can verify the legitimacy of receipts, estimate default rates, and implement risk management based on the electronic receipt system. In addition, platform clients can do batch docking, and the relevant hazards in the industrial chain will be discovered and identified efficiently.

Using blockchain technology, sensors and IoT devices linked to machines may be synced, leading to

more flexibility and cooperation with trading partners. Secure communication, secrecy, and transaction integrity are the primary benefits of this new feature. Transactions may be sent straight to a registered machine, allowing users to participate in on-demand manufacturing services. A wide variety of business logic might be included in blockchain-based decentralized consensus ledgers via a consensus mechanism, including payment terms, purchasing trends, intelligent inventory accuracy, preventive analytics, and maintenance.

Exchanging partners benefit from fresh and timely insights into their supply chain in real-time, with more accurate and trustworthy information about critical processes, events, and product attributes—such as quality—through the integrating decentralized ledger approach in the IoT platform. End-to-end traceability and quick product recalls are both possible with this IoT/Blockchain combination. Trading partners would be notified about the goods, possible dangers with preventative and corrective measures required to maintain a sufficient flow of reasonable production to the end consumers as a consequence.

3.1 Security Ratio

Companies are compelled to defend their information and data exchanges and the physical integrity of their products against theft and other unlawful trades, including aggravation and cloning, as supply chains become more complicated. Firms must keep up with the rapid development of covert and overt technologies to protect or monitor physical goods like products, containers, and palettes, along with logistics operations. Furthermore, IoT with distributed blockchain ledgers technology is being developed to increase quality and productivity and maintain the authenticity of supply-chain exchange partners. IoT and Blockchain technology has the potential to revolutionize a wide range of businesses since they can be used to manage IoT devices securely and efficiently. We may expect more responsive, resilient, and decentralized peer-to-peer monitoring system that is 'vulnerable to unauthorized access', private and real-time, when Blockchains and IoT are combined.

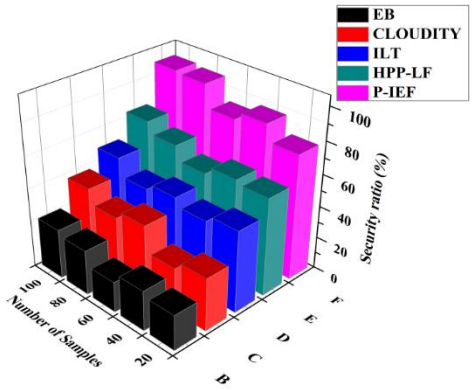

Figure 6. Security Ratio (%)

The security ratio (%) is featured in Fig 6. This decentralized ledger-based technology can transform the significant benefits of IoT. They serve as the bridge between gadget information interoperability b by guaranteeing privacy, confidentiality, and reliability. An IoT device's unique identity and trust management across devices, data lineage monitoring, authentication method, and traceability in IoT-based applications are some of the security concerns that blockchain solves. The blockchain system's decentralized strategy reduces the possibility of a single point of failure. To put it another way, the technology behind the blockchain helps to remove network security threats.

3.2 Scalability Ratio

Immutable transactions made possible via the combination of Blockchain and IoT devices boost supply chain automation and allow for better audit. Using Blockchain and IoT, supply chain partners benefit from secure and auditable information exchange via a tremendously diversified perspective framework. Using a network of linked IoT devices, the Blockchain platform might create an auditable and unchangeable history of transactions that is beneficial for item scalability, retrieval, and authenticity. Fig 7. exhibits the scalability ratio (%). As a result, sensor readings may create more confidence by combining real-time and immutable data into blockchain technology. IoT technology vendors are shifting their cloud-based services to Blockchain-based technology because of these qualities. IoT applications rely on real-time data, which has restricted blockchain capacity. Therefore these applications encounter difficulties in operating well. The scalability problem of blockchain technology has been addressed in several ways, including constructing more scalable consensus algorithms and designing private blockchains for IoT.

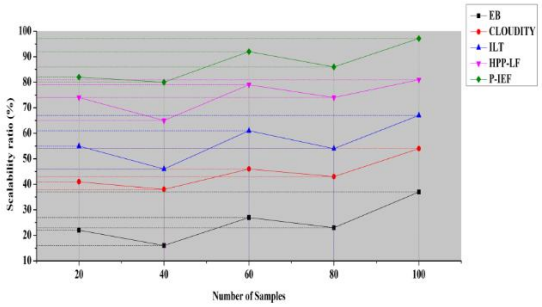

Figure7. Scalability Ratio (%)

3.3 Traceability Ratio

IoT devices and networks can be processed without interruption or human involvement, allowing transactions between devices to be carried out securely without interruption. Blockchain technology is already being used with tamper-evident smart contracts to verify the provenance and authenticity in the supply chain. It is impossible to replenish supply lines with a worst-quality

product because the corks are tagged.

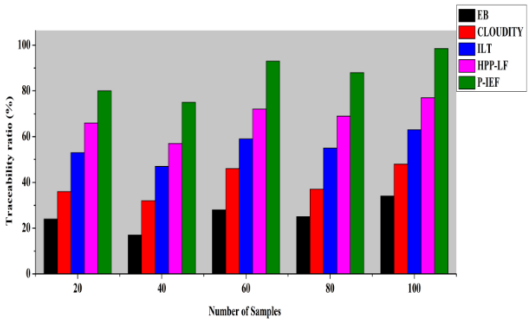

Figure 8. Traceability Ratio (%)

Fig 8. shows the traceability ratio (%). Customers can analyze the origin and history of their purchased items by registering their information on the ledger and cross-checking the traceability of their purchases with the product ID. A product's authenticity can only be verified confidence utilizing scientifically-based quantitative evaluation measures on the goods internally, instead of depending on hidden or explicit surveillance systems on the outside box. Blockchain and IoT are being used in several initiatives to improve traceability and interoperability. The privacy-assisted Information Exchange Framework offers a safe and seamless conversation between distributed ledgers and registries to boost supply chain transparency and quality management.

3.4 Efficiency Ratio

In multi-party supply chains, monitoring physical assets and products may be improved using blockchain technology. Any assets, goods, or merchandise related to a supply chain exchange partner's business will be made available to them. Firms can better govern their supply chains when they are aware of the movement of physical assets, natural resources or commodities, components, or finished goods. As a result, businesses make it easier for customers to get information about their products online or through mobile devices. It is possible to use a smartphone to scan the main wrapping of a product and retrieve crucial information and data stored on a blockchain. Allergens and components, provenance, process conditions, and transportation are just a few examples of information that might be included in this section. Using IoT sensors and ledger-based technology together in the cold chain to store and distribute perishable food goods is an excellent example of how IoT and blockchain technology can be used.

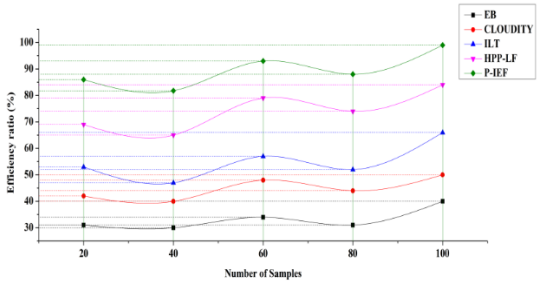

Figure 9. Efficiency Ratio (%)

Fig 9. illustrates the efficiency ratio (%). Machinery providers, parts replacement, and internet access providers might get share access to device information and give certifications with machinery to obtain higher efficiency, device management, and accessibility. Machine diagnostics, mutual recognition analytic methods, and interactions between machines and suppliers would enhance spare parts replacement and general maintenance procedures by integrating the ledger-based blockchain technology and the IoT.

3.5 Network Throughput Ratio

The IoT can improve the integrity of most immediate cloud transactions while simultaneously increasing throughput and decreasing latency. It can benefit from a multi-target approach. This work proposes a blockchain technique that concurrently analyses cloud computing rates and IoT throughput for IoT-enabled blockchain systems using a trusted model.

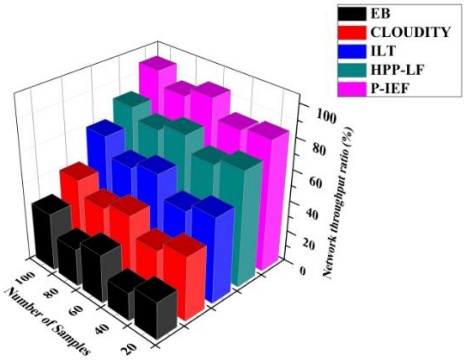

Figure 10. Network Throughput Ratio (%)

Network throughput ratio (%) is provided in Fig 10. The trust qualities and processing capacity of IoT nodes and controllers were created to improve the performance of software-defined supply chain systems. High-throughput demands may be met with low latency and security led to advances in industrial edge computing solutions for information exchange problems. This study effort to boost supply chain-weighted average cloud computing rate and transaction throughput is achieved.

4. Conclusions

Blockchain technology has been presented and

considered a possible solution to the problems faced by the retail business. When it comes to supply chain companies or loyalty programs, the progress of blockchain and how it may be used to create decentralized ledgers and smart contracts is discussed. This technology makes it possible to decrease the need for intermediaries, hence lowering transaction costs. Along with introducing blockchain technology and its many applications in retail, this paper discusses the problems firms face while using blockchain technology. It's expected that retail companies will begin using new blockchain technology to gain more transparency, better supply chain management, and trustworthy customer loyalty programs, leading to cost savings and increased consumer happiness. In the study, blockchain is presented as a method for securing access to IoT devices. Using blockchain's immutability, the blacklist of devices can be stored in the suggested paradigm. Using Blockchain and smart contracts overcomes the issue of not having a unique identification in the IoT.

6. Acknowledgement

This work was supported by Sehan University Research Fund in 2022.

References

[1]. H. Liu, Y. Zhang and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," IEEE Network, Vol.4, No. 32(3) pp. 78-83, Jun 2018. DOI: 10.1109/MNET.2018.1700344

[2]. M. Abdel-Basset, R. Mohamed, K. Sallam and M. Elhoseny, "A novel decision-making model for sustainable supply chain finance under uncertainty environment," Journal of Cleaner Production, Vol. 1;269:122324, Oct 2020. DOI:https://doi.org/10.1016/j.jclepro.2020.122324

[3]. S. Yousuf and D. Svetinovic, "Blockchain technology in supply chain management: Preliminary study," In2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) IEEE, Vol.22 (pp. 537-538) Oct 2019. DOI: 10.1109/IOTSMS48152.2019.8939222

[4]. Y. Luo, Q. Wei, Q. Ling and B.Huo, "Optimal decision in a green supply chain: Bank financing or supplier financing," Journal of Cleaner Production, Vol.20;271:122090, Oct 2020. DOI:https://doi.org/10.1016/j.jclepro.2020.122090

[5]. Yang, J.-P. . "A Novel Storage Virtualization Scheme for Network Storage Systems". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 1, Jan. 2022, pp. 08-13, doi:10.17762/ijritcc.v10i1.5514.

[6]. SK. Sahu, DP. Mohapatra, JK. Rout, KS. Sahoo and AK.Luhach, "An Ensemble-Based Scalable Approach for Intrusion Detection Using Big Data Framework," Big Data, Vol. 1;9(4):303-21, Aug 2021. DOI:https://doi.org/10.1089/big.2020.0201

[7]. DJ. Samuel and F.Cuzzolin, "Unsupervised anomaly detection for a Smart Autonomous Robotic Assistant Surgeon (SARAS) using a deep residual autoencoder," arXiv preprint arXiv:2104.11008-22. Apr 2021. DOI: 10.1109/LRA.2021.3097244

[8]. Chaudhary, D. S. . (2022). Analysis of Concept of Big Data Process, Strategies, Adoption and Implementation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 05–08. https://doi.org/10.17762/ijfrcsce.v8i1.2065

[9]. J. Su, X. Chu and S.Kadry, "Internet-of-Things-Assisted Smart System 4.0 Framework Using Simulated Routing Procedures," Sustainability, Vol. 12(15):6119, Jan 2020. DOI:https://doi.org/10.3390/su12156119

[10]. Saraireh, J., & Joudeh, H. (2022). An Efficient Authentication Scheme for Internet of Things. International Journal of Communication Networks and Information Security (IJCNIS), 13(3). https://doi.org/10.17762/ijcnis.v13i3.3422

[11]. K. Seyhan, TN. Nguyen, S. Akleylek and K.Cengiz, "Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey," Cluster Computing, Vol. 13:1-20, Aug 2021. DOI:https://doi.org/10.1007/s10586-021-03380-7

[12]. G. Amudha, "Dilated Transaction Access and Retrieval: Improving the Information Retrieval of Blockchain-Assimilated Internet of Things Transactions," Wireless Personal Communications, Vol. 6:1-21, Feb 2021. DOI:https://doi.org/10.1007/s11277-021-08094-y

[13]. Linda R. Musser. (2020). Older Engineering Books are Open Educational Resources. Journal of Online Engineering Education, 11(2), 08–10. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/41

[14]. J. Gao, H. Wang and H. Shen, "Task failure prediction in cloud data centers using deep learning," IEEE Transactions on Services Computing, Vol. 11, May 2020. DOI: 10.1109/TSC.2020.2993728

[15]. F. Wang, N. Yang, PM. Shakeel and V. Saravanan, "Machine learning for mobile network payment security evaluation system," Transactions on Emerging Telecommunications Technologies, Vol. 28:e4226, Jan 2021. DOI:https://doi.org/10.1002/ett.4226

[16]. BS. Rawal, G. Manogaran and M. Hamdi, "Multi-Tier Stack of Block Chain with Proxy Re-Encryption Method Scheme on the Internet of Things Platform," ACM Transactions on Internet Technology (TOIT), Vol. 22(2):1-20, Oct 2021. DOI:https://doi.org/10.1145/3421508

[17]. G. Amudha and P. Narayanasamy, "Distributed location and trust based replica detection in wireless sensor networks," Wireless Personal Communications, Vol. 102(4):3303-21, Oct 2018. DOI:https://doi.org/10.1007/s11277-018-5369-2

[18]. K. Seyhan, TN. Nguyen, S. Akleylek, K. Cengiz and SH.Islam, "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security," Journal of Information Security and Applications, Vol. 1;58:102788, May 2021.

DOI:https://doi.org/10.1016/j.jisa.2021.102788

[19]. XY. Liu, H. Yang, J. Gao and C. Wang, "FinRL: Deep reinforcement learning framework to automate trading in quantitative finance," Available at SSRN 3955949, Vol. 4, Nov 2021. DOI:https://doi.org/10.48550/arXiv.2111.09395

[20]. G. Manogaran, J. Ngangmeni, J. Stewart, DB. Rawat and TN. Nguyen, "Deep Learning-based Concurrent Resource Allocation for Enhancing Service Response in Secure 6G Network-in-Box Users using IIoT," IEEE Internet of Things Journal. Vol. 12, Oct 2021. DOI: 10.1109/JIOT.2021.3119336

[21]. R. Rajakumar, K. Sekaran, CH. Hsu and S.Kadry, "Accelerated grey wolf optimization for global optimization problems," Technological Forecasting and Social Change, Vol. 1;169:120824, Aug 2021. DOI:https://doi.org/10.1016/j.techfore.2021.120824

[22]. AA. Abd EL-Latif, B. Abd-El-Atty, SE. Venegas-Andraca and W.Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks," Future Generation Computer Systems, Vol. 1;100:893-906, Nov 2019. DOI:https://doi.org/10.1016/j.future.2019.05.053

[23]. S. Dey, S. Pal and V.Saravanan, "Computational Offloading with Deep Supervised Learning for Edge enabled IoT," InTechnological Advances in Science, Medicine and Engineering Conference 2021, Vol. 18, Jun 2021. DOI: 10.1109/JIOT.2020.2981557

[24]. M. Hader, A. El-Mhamedi, A. Abouabdellah, "Blockchain Integrated ERP for a Better Supply Chain Management," In2021 The 8th International Conference on Industrial Engineering and Applications (Europe), Vol. 8 (pp. 193-197), Jan 2021. DOI:10.1109/ICIEA49774.2020.9102084

[25]. C. Jiang and C. Ru, "Application of Blockchain Technology in Supply Chain Finance. In2020 5th International Conference on Mechanical," Control and Computer Engineering (ICMCCE) , Vol. 25 (pp. 1342-1345), Dec 2020. IEEE. DOI: 10.1109/ICMCCE51767.2020.00294

[26]. SR. Niya, D. Dordevic, AG. Nabi and T. Mann, "Stiller B. A platform-independent, generic-purpose and blockchain-based supply chain tracking," In2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) , Vol. 14 (pp. 11-12), May 2019. IEEE. DOI: 10.1109/BLOC.2019.8751415

[27]. Y. Yue and X.Fu, "Research on Medical Equipment Supply Chain Management Method Based on Blockchain Technology," In2020 International Conference on Service Science (ICSS), Vol. 24 (pp. 143-148), Aug 2020. IEEE. DOI: 10.1109/ICSS50103.2020.00030

[28]. M. Hölbl, M. Kompara, A. Kamišalić and L.Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," Symmetry. Vol. 10(10):470, Oct 2018. DOI:https://doi.org/10.3390/sym10100470

[29]. NN. Ahamed, TK. Thivakaran and P.Karthikeyan, "Perishable Food Products Contains Safe in Cold Supply Chain Management Using Blockchain Technology," In2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), (Vol. 1, pp. 167-172), Mar 2021. IEEE. DOI: 10.1109/ICACCS51430.2021.9442057