

Scalable and Secure Cloud-Based E-Commerce Supply Chain Management using Blockchain and Network Security

Mudassar Munir¹, Usman Ali Shah², Syed Atif Masroor³, Irfan Ali Shah⁴, Hafiz Muhammad Zubair Munir⁵

¹Senior IT Manager Digital Cooperation Organization, Riyadh, Saudi Arabia.
mmunir@dco.org

²Transportation Operations Manager Al Esnad Specialized Limited Company, Jeddah, Saudi Arabia.
usman.shah@profm.com.sa

³Senior Cloud and Infrastructure Specialist Maharah Human Resources Company, Riyadh, Saudi Arabia.
syed.masroor@projects.kafd.sa

⁴VP - Technology & CX, Maximus, Riyadh, Saudi Arabia. ishah@maximusgulf.com

⁵Assistant Manager Fleet & Transportation, Al Esnad Specialized Limited Company, Jeddah, Saudi Arabia.
mohammed.zubair@profm.com.sa

The rapid evolution of e-commerce has brought about increased complexity in supply chain operations, necessitating scalable, transparent, and secure systems. Traditional supply chains often face challenges such as data fragmentation, lack of trust among stakeholders, and vulnerabilities to cyber threats. This study proposes a scalable and secure cloud-based e-commerce supply chain architecture that integrates blockchain technology with network security protocols to address these issues effectively. The architecture employs a permissioned blockchain framework deployed on a cloud infrastructure to ensure decentralization, high availability, and seamless data access across the supply chain. Smart contracts automate order processing, shipment verification, and payment settlements. To enhance data integrity and prevent unauthorized access, the system incorporates robust network security mechanisms, including end-to-end encryption, multi-factor authentication, and anomaly detection. Evaluation results demonstrate improved transparency, reduced manual errors, and enhanced protection against tampering and cyberattacks. Cloud deployment enables dynamic scalability and facilitates real-time collaboration among manufacturers, warehouses, logistics providers, and consumers. This integrated approach not only strengthens trust and security in digital supply chain interactions but also supports the agility required for modern e-commerce platforms.

Keywords—Cloud Computing, E-Commerce, Supply Chain Management, Blockchain Technology, Network Security, Scalability.

I. INTRODUCTION

Supply chains have evolved into global networks that include manufacturers, intermediates, retailers, and consumers as a result of the expansion of online shopping [1]. The problems with traditional supply chain systems are many and serious, including inefficiency, fraud, counterfeiting, and a lack of

traceability. Overall supply chain management performance drops, customer happiness drops, and operational costs rise as a result of these problems. In recent years, cross-border e-commerce has grown rapidly, thanks to both economic globalisation and the advent of the Internet. Cooperation amongst members of the international supply chain is essential for the smooth operation of cross-border online commerce and delivery [2]. The importance of establishing reliable relationships among supply chain actors has grown in recent years [3]. The trust issue is difficult to resolve because of cultural, legal, and ideological disparities across countries [4]. By adopting cloud-based SCM, organizations gain alternative IT support through outsourcing, better integration, and reduced inconsistency of information. It also allows management of vast databases containing supplier and user data. However, cloud-based SCM (CSCM) also faces challenges, particularly concerning trust and security in data transmission between companies. Trust is a critical factor in CSCM as it enables flexibility, agility, and reduces transaction costs, thereby improving performance. Yet, maintaining trust remains difficult, and security issues further increase risks. To overcome these problems, Blockchain technology is introduced [5].

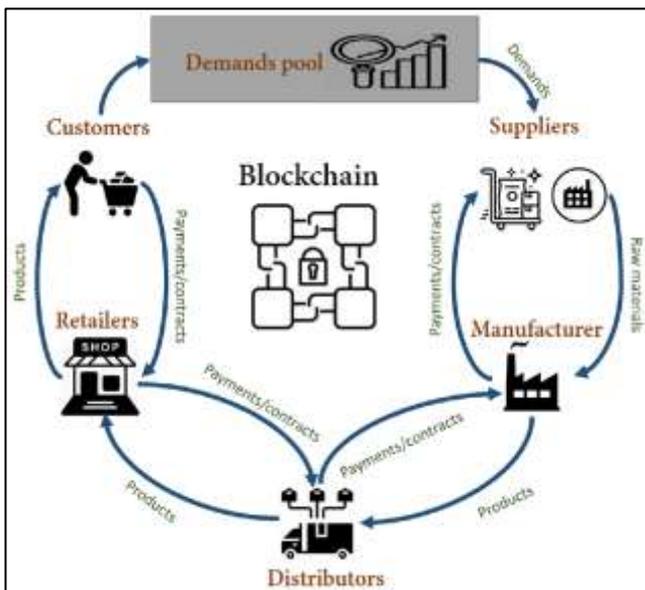


Fig.1. Supply chain process with Blockchain

A distributed public ledger, or blockchain, is a system for securely recording and tracking transactions online. To provide authenticity, access control, and identity verification, it employs encryption and digital signatures. Blockchain improves confidence between participants in supply chain management by allowing for tamper-proof data storage and end-to-end visibility. Integrating Blockchain into the supply chain model enhances CSCM's trustworthiness and security. [6]. This combination provides transparency, accountability, and secure data management across supply chain networks. Blockchain reduces transaction costs, improves monitoring without third-party interference, and ensures product quality during transport. It also guarantees secure data storage and introduces decentralized system architectures to enhance efficiency.

In this study, we present the Blockchain Enabled E-Commerce Supply Chain System (BEECSS), which integrates blockchain technology into the e-commerce supply chain to address these long-standing issues. Unlike previous approaches, BEECSS offers a fully automated supply chain using smart contracts, ensuring seamless communication and enforcement of terms between all participants [7]. By recording every transaction and event on an immutable ledger, BEECSS guarantees product authenticity and traceability, ultimately enhancing trust among both consumers and businesses.

II. LITERATURE SURVEY

The rapid expansion of e-commerce has led to increasingly complex supply chain networks, demanding scalability, transparency, and strong security mechanisms [8]. Traditional centralized systems [9] often face challenges such as data tampering, single points of failure, and lack of trust among stakeholders. Recent studies highlight the role of blockchain in ensuring decentralized trust, immutability, and traceability across supply chain transactions. At the same time [10], advanced network security techniques are being explored to safeguard sensitive data against cyber threats and unauthorized access. Integrating blockchain with secure cloud-based architectures provides a promising pathway toward scalable, transparent, and resilient e-commerce supply chain management. The 2022-2025 research study indicated the use of SCM in the cloud increases the cloud sector by 40%. This proves that cloud-enabled AI systems enhance scalability, agility, and collaboration. Blockchain technology has emerged as a transformative innovation in e-commerce supply chain management, offering unprecedented levels of transparency, security, and operational efficiency [11]. Several challenges to establishing the BC-SCM systems' reliability and security have been identified in the research. Most importantly, it draws attention to knowledge gaps that can lead to the BC-SCM's desired level of security [12]. There is an increase in risk due to the difficulty of establishing trust in SCM, which makes it difficult to sustain the function of the CSCM. Security concerns can also emerge from the CSCM's performance [13].

The Block Chain is used with CSCM [14] to get around these issues. The author in [15] presented blockchain intelligence and its function in the development of Web 3.0. In order to improve the capabilities of decentralised networks, the article lays out a framework for smart blockchains that incorporate cutting-edge AI methods. Possible uses in banking, SCM, and the Internet of Things are highlighted by the writers. In a similar vein, [16] investigated how the agri-food supply chain might benefit from blockchain technology to increase visibility. Improving traceability, reducing fraud, and ensuring food safety are all highlighted in the report [17]. Attacks pertaining to real businesses and assets have arisen as a result of the integration of blockchain technology into the supply chain [18]. The primary goal of every blockchain system should be to ensure the safety of all computing and communication processes [19]. Digital currency transactions between users in an unauthorised setting were successfully executed by blockchain [20].

TABLE I. SUMMARY OF LITERATURE ON BLOCKCHAIN-BASED SECURE E-COMMERCE SUPPLY CHAIN MANAGEMENT

Reference	Dataset	Methods	Results	Limitations
Yang et al. [21]	Simulated data; local Ganache private chain	Cloud + blockchain platform; bilateral matching model; smart contracts	Prototype supports secure info-sharing and supply-demand matching in automotive context.	Tested only on private chain with simulated data; lacks real-world deployment
Li et al. [22]	Simulated supply chains	CCChain architecture; hybrid blockchain; local data storage	Scalable, privacy-aware tracking; near-real-time tracking and tamper detection.	No real datasets; company-centric scope; unclear integration with cloud or security layers
Gao et al. [23]	Synthetic records	Chunked data + parallel search using bipartite graph and max matching	Time overhead reduced by up to 85%, with affordable storage overhead.	Using synthetic data; neglects network security and cloud integration
Kanaan et al. [24]	Prototype on Hyperledger Fabric	Zero-knowledge proofs (ZKRPs); smart contracts	Preserves provenance and privacy; minimal overhead shown on Fabric.	Fabric deployment only; not tested in cloud or real e-commerce scenarios

Ryan et al. [25]	Conceptual oil supply chain	Blockchain + smart contracts + IoT sensors framework	Framework improves traceability and security; supports reverse traceability.	Conceptual only; no empirical results or datasets; lacks evaluation in other domains
Yu et al. [26]	Simulated supply chains	Blockchain + cloud platform; smart contracts for transaction validation	Improves traceability, transparency, lowers reconciliation time, enhances data accuracy.	Abstract-level; no dataset details or performance metrics
Sharma et al. [1]	Simulated supply chains	Stackelberg game model; blockchain info platform (BIP)	Blockchain reduces misreporting, improves trust and purchasing metrics.	Theoretical model; assumes simplified two-level chain; no real data validation
Zhu et al. [2]	Simulated supply chains	Literature review on scalability, privacy, security, protocols	Highlights scalability solutions (sharding, off-chain); privacy-preserving smart contracts; identifies challenges.	Lacks empirical data; mostly conceptual and broad review
Harikrishna et al. [4]	Simulated supply chains	Technical evaluation of blockchain challenges	Details block size constraints, scalability, privacy, interoperability issues.	Broad survey; lacks applied system or real dataset analysis

At a digital currency seminar organised by the People's Bank of China, participants discussed the potential benefits of using blockchain technology to create digital currency. The seminar looked at blockchain literature from 2014 to 2018 and concluded that, theoretically, methodologically, and empirically speaking, blockchain research is still in its early stages [4]. Financial exclusion, improper banking products, exorbitant costs, and a lack of financial literacy were listed as four problems that blockchain technology might alleviate, according to the study [4]. This proved that increasing the size of an enterprise's assets is a key motivator for using blockchain technology, and that doing so improves asset turnover rate and decreases sales expense rate.

III. METHODOLOGY

The methodology focuses on developing a scalable and secure cloud-based e-commerce supply chain management framework by leveraging blockchain and network security. The approach begins with data collection, where the Kaggle e-commerce supply chain dataset is pre-processed and enriched with derived features. The proposed system architecture integrates blockchain, cloud, and security layers for end-to-end management. Blockchain integration ensures immutable recording of transactions, while the cloud layer provides scalability and efficient storage for high transaction volumes. Finally, network security mechanisms safeguard confidentiality, integrity, and trust, enabling a transparent, tamper-resistant, and resilient supply chain framework.

A. Dataset Description

This study utilizes the E-commerce order & supply chain dataset from Kaggle [2, 6, 17], which consists of five interconnected tables: orders, order items, customers, Payments, and products providing a complete view of e-commerce activities. The orders table captures purchase, approval, and delivery timestamps, enabling computation of fulfillment times, approval delays, and delivery deviations. Order items link each order to specific products with details such as seller id, price, and shipping charges, supporting item-level revenue and logistics analysis. Customer data, including geographic attributes, allows regional demand assessment and repeat-purchase identification, while the Payments table facilitates installment and settlement flow analysis. The products table, with category and dimensional

Fig.1. Proposed model block diagram

The efficiency of the system can be quantified using several performance equations. The order fulfillment time (OFT) is expressed as:

$$OFT = T_{\text{delivered}} - T_{\text{purchase}} \tag{1}$$

which calculates the duration between order placement and delivery, reflecting supply chain responsiveness. Another key metric is the delivery delay (DD), given by:

$$DD = T_{\text{delivered}} - T_{\text{estimated_delivery}} \tag{2}$$

indicating whether an order was delivered earlier or later than expected. To evaluate the financial dimension, the total order value (TOV) is computed as:

$$TOV = \sum_{i=1}^n (P_i + S_i) \tag{3}$$

where P_i denotes the price of item i and S_i the shipping charges, capturing the overall worth of a transaction. On the blockchain side, the storage overhead (BSO) can be modeled as:

$$BSO = \frac{S_{\text{block}}}{N_{\text{orders}}} \tag{4}$$

which measures the average storage consumed per order when events are immutably logged on the ledger. Finally, system performance is reflected in transaction throughput (TPS), defined as:

$$TPS = \frac{N_{\text{tx}}}{T_{\text{end}} - T_{\text{start}}} \tag{5}$$

representing the number of transactions successfully processed per second. Collectively, these equations capture operational efficiency, delivery performance, financial flows, blockchain scalability, and overall system robustness.

C. Blockchain in Network Security

The Blockchain-Enabled E-commerce Supply Chain System (BEECSS) enhances transparency and trust by securely recording every transaction as an immutable block in a distributed ledger. This decentralized design eliminates dependence on centralized intermediaries, reducing risks of fraud and manipulation. Each block is cryptographically linked to the previous one, making it computationally infeasible to alter past records without consensus from the network. Transactions are validated using consensus mechanisms such as Proof-of-Work, Proof-of-Stake, or Byzantine Fault Tolerance, ensuring integrity and authenticity. By combining encryption with distributed validation, blockchain establishes a mathematical trust model that guarantees secure, verifiable, and tamper-resistant e-commerce supply chain operations.

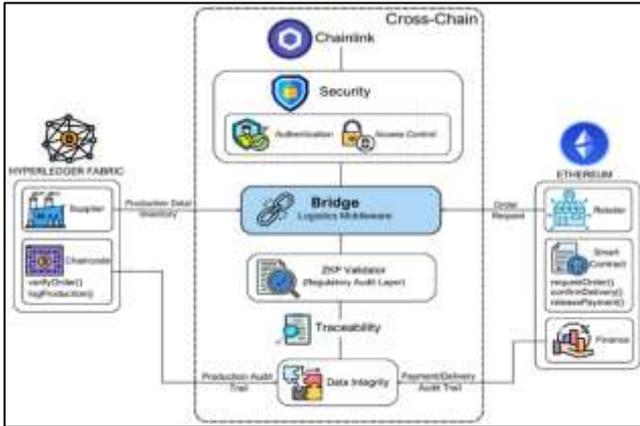


Fig.3. Blockchain-Enabled Supply Chain Management

$$P(\text{ Tampering Success }) = \left(\frac{1}{N}\right)^k \tag{6}$$

where N is the total number of validating nodes, and k is the number of confirmations required. As k increases, the probability of successful tampering approaches zero. Blockchain also introduces transactional transparency, as all participants can view and verify activities without compromising confidentiality. This can be represented using an auditability function:

$$T = \sum_{i=1}^n \log (\text{ Transaction } _i) \tag{7}$$

where T is the complete traceable audit trail, and every Transaction $_i$ is permanently recorded in the ledger. In addition to transparency, blockchain ensures integrity and accountability through cryptographic hashing. If a block contains a transaction set X, its hash H(X) guarantees that even a minor modification produces a completely different result:

$$H(X) \neq H(X') \text{ for any } X' \neq X \tag{8}$$

This immutability simplifies dispute resolution since all parties can verify the exact state of the supply chain at any given point. Blockchain ensures data integrity by storing data in an immutable ledger where each transaction is verified and linked to the previous block.

$$h(x) = H(m) \tag{9}$$

Here, H is a cryptographic hash, m is transaction data, and h(x) is the hash output. Any change in m alters h(x), making tampering evident. Authentication is decentralized using cryptographic keys:

$$C = E_{K_{pub}}(M), M = D_{K_{priv}}(C) \tag{10}$$

This ensures identity verification without a central authority, reducing risks of theft and enhancing privacy. Secure transactions are validated through digital signature.

$$S = E_{K_{priv}}(h(m)), h(m) \stackrel{?}{=} D_{K_{pub}}(S) \tag{11}$$

Consensus mechanisms such as Proof of Work follow:

$$H(\text{ nonce } \parallel \text{ data }) < T \tag{12}$$

Smart contracts further improve reliability by executing agreements automatically when conditions are met. Together, these features strengthen data integrity, authentication, and transaction security, enhancing resilience against cyber threats in supply chains and e-commerce.

D. Cloud Layer for Scalability

In blockchain-enabled e-commerce supply chains, scalability challenges arise due to limited on-chain storage and computation. To overcome this, a Distributed Blockchain Cloud (DBC) architecture integrates the IoT device layer, fog blockchain layer, and cloud blockchain layer. The system employs two mapped chains: the Reputation Blockchain (RBC) at the fog layer and the Information Blockchain (IBC) in the cloud. IoT devices feed raw data to fog nodes, which generate lightweight reputation blocks capturing trust scores of participants, while detailed transaction and product data are stored as long IBs in the cloud. Node classification balances resource use, with full, light, and basic nodes sharing tasks. Smart contracts further ensure integrity by detecting inconsistencies between RBC trust values and IBC records. When IoT and fog data are offloaded to the cloud, only their cryptographic hashes are stored on-chain to guarantee verifiability:

$$H(D_{IBC}) = h_{IBC}, H(D_{RBC}) = h_{RBC} \quad (13)$$

where D_{IBC} and D_{RBC} represent datasets stored in the cloud and fog layers, and h are their corresponding hashes recorded on the blockchain. Any mismatch between recomputed and stored hashes indicates tampering or unauthorized modification. To handle large-scale operations, elastic cloud resources dynamically increase processing capacity (μ), ensuring that the system load factor (ρ) remains below 1 ($\rho < 1$), even during peak e-commerce demand. This prevents congestion and maintains system responsiveness.

IV. RESULTS

Simulation experiments were conducted to evaluate the performance of the proposed cloud-based blockchain-enabled e-commerce supply chain system on a test computer with Intel Core i5-7300HQ CPU, 16 GB RAM, and a 64-bit operating system. The evaluation focuses on computation costs across the three main stages of the framework: Registration, Product Circulation, and Record Validation. The Product Circulation stage is further divided into four sequential steps, reflecting end-to-end supply chain operations. Results indicate that computation costs are practical and efficient, demonstrating that the hybrid cloud–fog architecture can handle real-time processing of IoT-enabled supply chain data without overloading the blockchain network. The cloud layer provides scalable storage and computation for long Information Blockchain (IBC) records, while the fog layer supports low-latency trust verification via Reputation Blockchain (RBC) blocks. This layered architecture ensures rapid validation at the edge and elastic cloud processing for large-scale datasets. Transaction throughput (TPS) analysis confirms the suitability of the system for high-volume operations. Cloud-assisted blockchain execution enables peak scalability while maintaining network stability. Decentralization and security assessments show that the mapped IBC–RBC structure, combined with smart contracts for automated verification and misbehaviour detection, ensures reliable, tamper-resistant operations. The system effectively balances performance, trust, and resource efficiency, confirming that integrating cloud elasticity with blockchain immutability provides a robust, secure, and scalable foundation for modern e-commerce supply chain management.

Our suggested system is practical, efficient, and requires less computing power, as seen in the experimental results (Figure 4). Performing product record validation in a single supply chain takes just 1.335 seconds for a merchant.

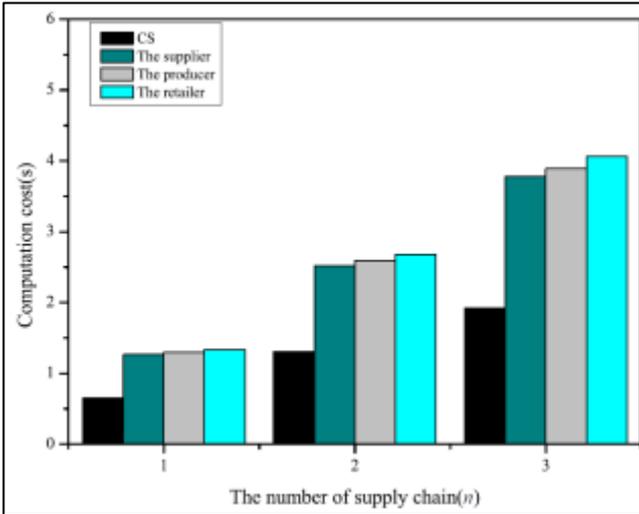


Fig.4. The computation cost of validation

When a client requests data from the server using an API, the server responds in formats such as JSON, XML, HTML, or TEXT, depending on the requirements and the request method employed. The execution time of the request and the response duration vary according to the volume of data being transmitted. For instance, requests involving records ranging from 100 to 10,000 illustrate clear execution time patterns, where larger datasets result in longer response times. A detailed analysis of the retrieved data and performance observations is presented in Figure 5.

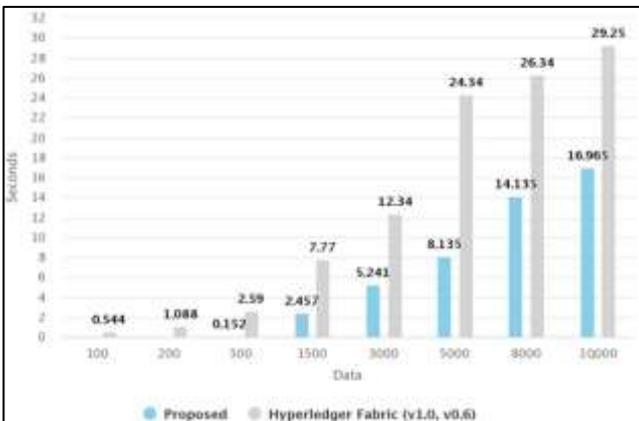


Fig.5. Execution time of overall records

While the query function shows variations, the invoke function shows no substantial difference in the execution durations of the two queries. The two implementations' invoke function execution times are shown in Figure 6. It should be noted that the query function includes retrieving all data from the database into memory, while the invoke function involves providing data to the client over time.

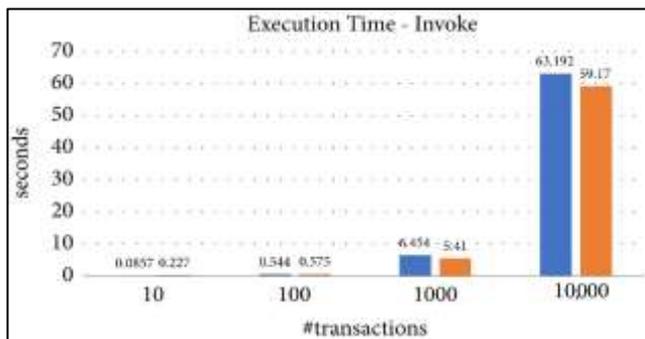


Fig.6. Execution time for both queries in invoke function

Figure 7 compares decentralization across blockchain platforms, showing Ethereum as most decentralized, ensuring transparency and trust. Binance Smart Chain and Solana balance speed with fewer validators, while Hyperledger Fabric remains centralized, suiting enterprise supply chains requiring permissioned control and efficiency.

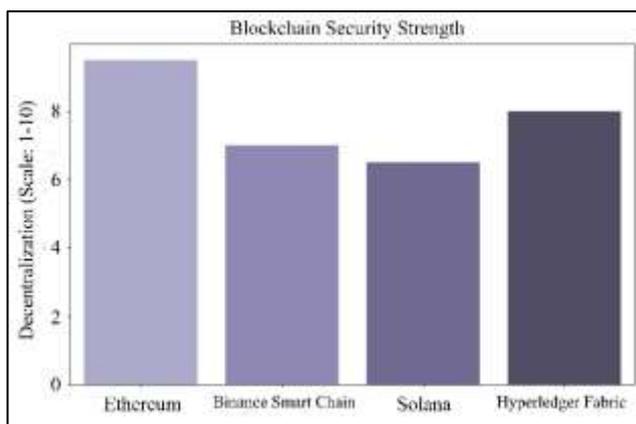


Fig.7. Blockchain Decentralization Comparison

The proposed BEECSS, integrated with cloud infrastructure, enhances customer experience through real-time tracking and transparent issue resolution. Customers gain complete visibility over their orders, with the ability to track shipments in real time and anticipate delivery timelines accurately. Additionally, the system efficiently manages complaints and returns, fostering higher customer satisfaction and loyalty. Despite these advantages, challenges remain in integrating blockchain with legacy systems and scaling the framework for large-scale e-commerce operations. Future enhancements will optimize large-scale deployment, automate complex supply chain workflows, and ensure interoperability with other systems. By addressing these challenges, BEECSS can deliver a secure, transparent, and innovative ecosystem for global trade.

V. CONCLUSION

Integrating blockchain with cloud-enabled e-commerce supply chains transforms traditional systems by enhancing transparency, security, and operational efficiency. The blockchain enabled e-commerce supply chain management System records all events from order placement to delivery and payment on an immutable ledger, providing stakeholders with real-time, verifiable updates. Cloud resources ensure scalable storage and computation, handling large transaction volumes while enabling low-latency analytics and smart contract execution. This combination reduces manual effort, mitigates fraud, accelerates transactions, and simplifies compliance. Challenges such as scalability, system integration,

and environmental impact remain, but solutions like energy-efficient consensus mechanisms and hybrid cloud-blockchain architectures can address them. Future research will focus on optimizing performance, privacy, and interoperability with technologies like IoT and AI, driving secure, efficient, and sustainable global supply chain.

REFERENCES

- [1] Sharma, A. (2025). Integrating Blockchain Technology in Cloud Computing: Enhancing Security and Transparency. *Recent Trends in Computer Science and Software Technology*, 10(1).
- [2] Zhu, Y. (2025, March). Integration of Blockchain Technology, International Trade and Information Security: A Systematic Study. In *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)* (pp. 1598-1603). IEEE.
- [3] Madasamy, S., Rajendran, P., Prasad, K. V. S., Rajendiran, M., Sathyakala, S., & Maranan, R. (2025). Implementation of customer engagement in e-commerce with smart transactions through direct marketing using blockchain technology and cloud computing techniques. In *Hybrid and Advanced Technologies* (pp. 345-350). CRC Press.
- [4] Hari Krishnan, S., Gopikrishnan, R., & ML, S. K. (2025, April). Quantum-Secured E-Commerce with Blockchain, BB84 and BLAKE3 Encryption Using GNN. In *2025 International Conference on Inventive Computation Technologies (ICICT)* (pp. 1889-1896). IEEE.
- [5] Thayyaba Khatoun Mohammed, D N Vasundhara, Syeda Husna Mehanoor, E. Sreedevi, Puranam Revanth Kumar, CH Manihass, Shaik Fareed Baba "A Novel Fusion Approach for Advancement in Crime Prediction and Forecasting using Hybridization of ARIMA and Recurrent Neural Networks", *Journal of Information Systems Engineering and Management*, Vol. 10, Issue 38, pp. 404-420, 2025.
- [6] Puranam Revanth Kumar, Gouse Baig Mohammad, Pallati Narsimhulu, Dharmisha Narasappa, Lakshmana Phaneendra Maguluri, Subhav Singh, Shitharth Selvarajan, "Computer Modeling Approaches for Blockchain-Driven Supply Chain Intelligence: A Review on Enhancing Transparency, Security, and Efficiency", *Computer Modeling in Engineering & Sciences*, pp. 1-40, 2025.
- [7] B Shilpa, Puranam Revanth Kumar, and Rajesh Kumar Jha, "LoRa DL: a deep learning model for enhancing the data transmission over LoRa using autoencoder", *The Journal of Supercomputing*, vol. 79, pp. 17079 –17097, 2023.
- [8] Maheshwaran, T., Muthumariakshmi, S., Suganya, K., Maheswari, B., & Girija, P. (2024). Securing E-Commerce Strategies With Cloud, Blockchain, AI, and ML. In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning* (pp. 470-500). IGI Global.
- [9] Roop Ranjan, Dilkeswar Pandey, Ashok Kumar Rai, Deepak Gupta, Pawan Singh, Puranam Revanth Kumar, and Sachi Nandan Mohanty, "A Manifold-Level Hybrid Deep Learning Approach for Sentiment Classification Using an Autoregressive Model", *Applied Sciences*, vol. 13, no. 5, p.3091, 2023.
- [10] N. Arivazhagan, K. Somasundaram, Gouse Baig Mohammad, Puranam Revanth Kumar et al., "Cloud-Internet of Health Things (IOHT) Task Scheduling Using Hybrid Moth Flame Optimization with Deep Neural Network Algorithm for E Healthcare Systems", *Scientific Programming*, Volume 2022, Article ID 4100352, pp. 1-12, 2022.
- [11] Doğan, Ö., & Karacan, H. (2023). A blockchain-based e-commerce reputation system built with verifiable credentials. *IEEE Access*, 11, 47080-47097.
- [12] Pranto, T. H., Noman, A. A., Rahaman, M., Haque, A. B., Islam, A. N., & Rahman, R. M. (2022). A blockchain, smart contract and data mining based approach toward the betterment of e-commerce. *Cybernetics and Systems*, 53(5), 443-467.
- [13] Gouse Baig Mohammad, Shitharth, and Puranam Revanth Kumar, "Integrated Machine Learning Model for an URL Phishing Detection", *International Journal of Grid and Distributed Computing*, vol. 14, Issue 1, pp: 513-529, 2021.
- [14] Puranam Revanth Kumar, and T Ananthan "Machine Vision using LabVIEW for Label Inspection", *Journal of Innovation in Computer Science and Engineering (JICSE)*, Vol.9, Issue 1, pp: 58 - 62, 2019.
- [15] ZhuanSun, F., Chen, J., Chen, W., & Sun, Y. (2021). The Mechanism of Evolution and Balance for e-Commerce Ecosystem under Blockchain. *Scientific Programming*, 2021(1), 5984306.
- [16] B Shilpa, Puranam Revanth Kumar, Rajesh Kumar Jha, "Spreading Factor Optimization for Interference Mitigation in Dense Indoor LoRa Networks", *IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, pp. 1-5, 2023.
- [17] Puranam Revanth Kumar "Position Control of a Stepper Motor using LabVIEW" *3rd International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, pp. 1551 - 1554, 2018.
- [18] Guan, Z., Wang, N., Fan, X., Liu, X., Wu, L., & Wan, S. (2020). Achieving secure search over encrypted data for e-commerce: a blockchain approach. *ACM Transactions on Internet Technology (TOIT)*, 21(1), 1-17.
- [19] Puranam Revanth Kumar and B. Shilpa, "An IoT-Based Smart Healthcare System with Edge Intelligence Computing", *Reconnoitering the Landscape of Edge Intelligence in Healthcare*, CRC Press, pp. 31-46, 2024.

- [20] Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2019, December). Cloud based supply chain management system using blockchain. In 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT) (pp. 390-395). IEEE.
- [21] Yang, C. N., Chen, Y. C., Chen, S. Y., & Wu, S. Y. (2019, March). A reliable e-commerce business model using blockchain based product grading system. In 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA) (pp. 341-344). IEEE.
- [22] Li, M., Shen, L., & Huang, G. Q. (2019). Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. *Computers & Industrial Engineering*, 135, 950-969.
- [23] Gao, F. (2019). Data encryption algorithm for e-commerce platform based on blockchain technology. *Discrete & Continuous Dynamical Systems-Series S*, 12.
- [24] Kanaan, R. K., Abumatar, G., Hussein, A. M. A., & Al-Lozi, M. (2019). Management information system using blockchain technology in an e-commerce enterprise: A systematic review. *Journal of Business & Management (COES&RJ-JBM)*, 7(3), 216-233.
- [25] Ryan, P. A. (2017). Smart contract relations in e-commerce: legal implications of exchanges conducted on the blockchain. *Technology Innovation Management Review*.
- [26] Yu, Y., Wang, X., Zhong, R. Y., & Huang, G. Q. (2016). E-commerce logistics in supply chain management: Practice perspective. *Procedia Cirp*, 52, 179-185.