International Journal of Advanced Scientific Innovations Volume 05 Issue 08, August 2023
ISSN: 2582-8436

Impact of IoT and Cloud Computing on Enterprise Supply Chain Security Management

Shambulingappa H S, Rashmi T V

shambu.hs13@gmail.com, rashmi.tv@eastpoint.ac.in

Abstract – ***At the enterprise level of supply chain security management, the impact of network technologies such as the Internet of Things (IoT) and cloud computing has been substantial. These technologies have influenced various aspects of supply chain management, including operational modes and security management methods. Traditional supply chain management relied on outdated communication methods and manual interventions for decision-making and processing. In contrast, modern information and communication technologies offer immediacy and strong correlation. This article leverages IoT data interconnection technology to construct supply chain management models, incorporating efficient cloud computing algorithms. The exploration of supply chain security management models encompasses participant perspectives, activity modes, and module operations, with subsequent data comparisons. Experimental results reveal an average accuracy of approximately 89.60% and a remarkable prediction accuracy of 98.48% for benefits. Stability testing demonstrates an average stability of around 96.02% after multiple iterations. The research highlights the significant application potential of IoT and cloud computing technologies in enhancing supply chain security management, providing enterprises with more effective tools for this purpose.***

Keywords — Enterprise, Supply Chain Security Management, Internet of Things (IoT), Cloud Computing, Operational Modes, Security Management Methods, Data Interconnection Technology

I. INTRODUCTION

China's economy continues to evolve, the supply chains of enterprises are becoming increasingly complex and expansive due to both internal factors in China and the global trend of globalization. This growing complexity has led to heightened security risks in supply chain management, necessitating enterprises to prioritize and implement effective security measures. Traditional supply chain models, relying on outdated communication methods and manual interventions, are inadequate in addressing the interconnected and interdependent nature of modern supply chains. The rising degree of networking in supply chains makes them vulnerable to various security vulnerabilities and threats.

In response to these challenges, enterprises must concentrate on supply chain security management and devise corresponding security measures. These measures encompass implementing background checks on suppliers, enhancing physical security measures, strengthening information security, and establishing a robust risk management system.

The creation of a supply chain security management model is crucial for enterprises to comprehensively identify and mitigate potential threats. The interconnected nature of supply chain links requires a thorough evaluation of each link to minimize security risks in logistics, manufacturing, sales, and other aspects. Scholars have conducted diverse research studies on supply chain security management models, employing approaches like the Kraljic Portfolio Purchasing Model and strategies focusing on regional collaborative development, supply chain security system construction, and core technology breakthroughs.

In the era of big data, scholars underscore the impact of the big data era on supply chain security management, considering operational modes, methods, and security. The expanding coverage of the Internet of Things (IoT) further contributes to the interconnection of facilities, equipment, and networks among multiple parties. IoT devices, supported by cloud computing, facilitate real-time monitoring, data processing, analysis, and storage, offering intelligent and convenient services for constructing a supply chain security management system.

This article endeavors to construct an information and communication technology supply chain security management model based on the Internet of Things and cloud computing technology. It delves into application scenarios, scrutinizes the existing problems of IoT and cloud computing technology in supply chain security management, and devises a model enabling real-time monitoring and analysis. The model aims to enhance manageability, transparency, and data flow security in the supply chain. With the backing of cloud computing, this model enables centralized storage and analysis of supply chain information, establishing an information security guarantee system to effectively counter security threats. The article provides valuable insights for enterprises involved in digital supply chain security management.

II. CONSTRUCTION OF THE MODEL

This platform assumes responsibility for overseeing the security management of the entire supply chain, incorporating tasks such as supplier data review, audits, and scans leveraging cutting-edge technologies. It ensures real-time monitoring of the supply chain and encompasses various modules, such as supplier relationship management, supply chain security protocol evaluation, and historical impact factors. The goal is to shield enterprises from vulnerabilities and attacks within the supply chain.

The competitive capability of participating suppliers within the supply chain is refined through this model, considering factors like the construction of the supplier quality certification system, historical qualification rate, product price change rate, and more. Multiple evaluation indicators, analyzed and predicted through algorithms, serve as a decision-making basis for the secure and stable operation of the supply chain.

Logistics management is deemed crucial in the supply chain, prompting the establishment of an Internet of Things (IoT) connection across the entire logistics chain. The IoT platform facilitates real-time monitoring of logistics processes, information provision, and order tracking while ensuring the integrity and confidentiality of the shared information.

Building an IoT information link in the supply chain involves establishing evaluation contracts at each node. Distinct contract strategies are implemented for entities in multiple supply chain nodes, considering their characteristics. These contracts enable real-time information exchange, behavior supervision, and guarantees for supply chain security management under information and communication technology. Various IoT nodes are established in the IoT link network to monitor real-time information across logistics, warehousing, production, processing, transportation, and sales links. Feedback on each node's information, such as on-time completion rate and logistics arrival rate, is processed, and algorithmic allocation through evaluation contracts is recorded in the evaluation relationship database. This provides a foundational calculation for the operation of the supply chain security management model.

III. EXPERIMENT

Cloud computing serves as a vital resource in the supply chain by offering data storage and processing capabilities, supporting operations and decision-making processes. It plays a crucial role in allocating key resources, facilitating data analysis, and aiding enterprises in addressing supply chain risks and challenges. This enhances the competitiveness and reliability of the supply chain, providing features like dynamic configuration, network traffic control, and security auditing.

When establishing an evaluation relationship database and a supply chain security management model, principal component analysis is applied to the characteristic information of the supply chain operation process. Different data sub-blocks are created at various levels of the feedback supplier information elements. The original data space in the IoT information network, comprising characteristic attributes, is divided into multiple sub-blocks. Methods like independent component analysis and principal component analysis are utilized to extract information features from each data sub-block, emphasizing dimensionality reduction and diversity requirements for sub-block partitioning.

Supply chain security management is a critical task for protecting the interests of enterprises and consumers. Establishing a comprehensive experimental indicator system is essential for evaluating, monitoring, and enhancing supply chain security. The supply chain security management model, based on the Internet of Things and cloud computing technology, ensures the secure flow of goods and information in the supply chain. The security chain management platform serves as the central component in this model, with other elements positioned around it. The Internet of Things and cloud computing enhance the connectivity and capabilities of the security chain platform. The experimental model relies on evaluation indicators, using simulated original data for testing accuracy in supply chain stability trend prediction and iterative stability testing through multiple operations.

IV. RESULTS

It is evident that the data feedback effects on model testing and samples vary due to different subject objects in the supply chain. The overall average accuracy for stable trend prediction is approximately 89.60%, displaying slight differences among various elements. Notably, partners in the supply chain exhibit higher accuracy in most evaluation indicators compared to suppliers, manufacturers, and distributors, with a baseline exceeding 90%. The benefit prediction accuracy reaches a remarkable 98.48%. This underscores the pivotal role of partners as key nodes in the supply chain, influenced by factors like contracts and historical cooperation, contributing to their significant position in supply chain security management. Partners exhibit efficient characteristics with fewer interference factors and more potential benefits.
On the other hand, manufacturers, acting as intermediate nodes between suppliers and distributors, demonstrate relatively lower accuracy values in the testing of supply chain security management models. The accuracy of trend prediction for manufacturers typically ranges between 80%

and 90%, indicating that manufacturers face various factors in the supply chain management process, resulting in a less accurate prediction of stable trends. To address this, leveraging information communication technology, along with the advantages of cloud computing and the multi-party interconnection characteristics of the Internet of Things, becomes crucial for manufacturers to enhance timely and effective information communication, reducing unstable trends in supply chain security management.

In the stability testing of the supply chain security management model, multiple iterations are employed to analyze the situations faced by various entities in the supply chain nodes, determining the stability trend of the model operation. The overall average stability level after multiple iterations is around 96.02%. Manufacturers exhibit relatively larger stability fluctuations, with approximately a 4-percentage point fluctuation, while other nodes generally fluctuate around 3%. These accuracy and stability tests provide preliminary experimental data for the supply chain security management model, allowing the determination of its basic effectiveness during operation. Additionally, the model can undergo user testing, functional testing, usability testing, and security testing to ensure its feasibility, effectiveness, and security in practical operations.

V. CONCLUSION

Leveraging the capabilities of the Internet of Things (IoT) and cloud computing has highlighted the increasing benefits of information and communication technology in supply chain security management. The development of a supply chain security management model for information and communication technology based on the Internet of Things and cloud computing is a significant area of research. This study integrates IoT technology and cloud computing methodologies to establish a comprehensive supply chain security management model, encompassing critical aspects such as risk prediction, identification, analysis, and governance. Through continuous iterative refinement, the model effectively manages information security risks in the supply chain. The article further conducts a comparative analysis of the advantages of IoT and cloud computing technology, employing a series of security management strategies and mechanisms to address prevalent information security issues in the supply chain. This model enables the effective management of IoT and cloud computing technology security in enterprise information communication supply chains, thereby enhancing information security levels and competitiveness. It is important to note that the model's construction process focuses solely on algorithm simulation testing of IoT and cloud computing advantages and lacks practical exploration in specific applications and user feedback. Subsequent research should enhance the model by incorporating more influencing factors and testing its impact in complex environments, offering opportunities for further improvement

REFERENCES

[1] Roberto Brandín, Sepehr Abrishami, IoT-BIM and blockchain integration for enhanced data traceability in offsite manufacturing, Automation in Construction, Volume 159, 2024, 105266, ISSN 0926-5805, https://doi.org/10.1016/j.autcon.2024.105266.

[2] Kamalendu Pal, Ansar-Ul-Haque Yasar, Internet of Things Impact on Supply Chain Management, Procedia Computer Science, Volume 220, 2023, Pages 478-485, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.03.061.

[3] Mani Deep Karumanchi, J.I. Sheeba, S. Pradeep Devaneyan, Integrated Internet of Things with cloud developed for data integrity problems on supply chain management, Measurement: Sensors, Volume 24, 2022, 100445, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2022.100445.

[4] Soujanya Mantravadi, Jagjit Singh Srai, How Important are Digital Technologies for Urban Food Security? A Framework for Supply Chain Integration using IoT, Procedia Computer Science, Volume 217, 2023, Pages 1678-1687, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.368.

[5] Soonh Taj, Ali Shariq Imran, Zenun Kastrati, Sher Muhammad Daudpota, Raheel Ahmed Memon, Javed Ahmed, IoT-based supply chain management: A systematic literature review, Internet of Things, Volume 24, 2023, 100982, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100982.

[6] Cui Wang, Huifang Zhang, Construction of Supply Chain Security Management Model for Information and Communication Technology Based on the Internet of Things and Cloud Computing, Procedia Computer Science, Volume 228, 2023, Pages 745-754, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.11.088.

[7] Abdullah Lakhan, Qurat-Ul-
in Mastoi, Mohamed Elhoseny, Muhammad
Suleman Memon & Mazin Abed Mohammed (2022) Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud, Enterprise Information Systems, 16:7, DOI: 10.1080/17517575.2021.1883122

[8] Mohsen Attaran (2020) Digital technology enablers and their implications for supply chain management, Supply Chain Forum: An International Journal, 21:3, 158-172, DOI: 10.1080/16258312.2020.1751568

[9] Sheshadri Chatterjee, Arpan Kumar Kar & Syed Ziaul Mustafa (2021) Securing IoT devices in smart cities of India: from ethical and enterprise information system management perspective, Enterprise Information Systems, 15:4, 585-615, DOI: 10.1080/17517575.2019.1654617

[10] Julius
H. Boehmer, Manish Shukla, Dharm Kapletia & Manoj Kumar Tiwari (2020) The impact of the Internet of Things (IoT) on servitization: an exploration of changing supply

relationships, Production Planning & Control, 31:2-3, 203-219, DOI: 10.1080/09537287.2019.1631465

[11] Zachary A. Collier & Joseph Sarkis (2021) The zero trust supply chain: Managing supply chain risk in the absence of trust, International Journal of Production Research, 59:11, 3430-3445, DOI: 10.1080/00207543.2021.1884311

[12] Ianire Taboada & Himanshu Shee (2021) Understanding 5G technology for future supply chain management, International Journal of Logistics Research and Applications, 24:4, 392-406, DOI: 10.1080/13675567.2020.1762850

[13] Petri Helo & Yuqiuge Hao (2022) Artificial intelligence in operations management and supply chain management: an exploratory case study, Production Planning & Control, 33:16, 1573-1590, DOI: 10.1080/09537287.2021.1882690

[14] Hajar Fatorachian & Hadi Kazemi (2021) Impact of Industry 4.0 on supply chain performance, Production Planning & Control, 32:1, 63-81, DOI: 10.1080/09537287.2020.1712487

[15] Malin Song, Ron Fisher, Ana Beatriz Lopes de Sousa Jabbour & Ernesto D.R. Santibañez Gonzalez (2022) Green and sustainable supply chain management in the platform economy, International Journal of Logistics Research and Applications, 25:4-5, 349-363, DOI: 10.1080/13675567.2022.2045763