

Developing an Information and Communication Technology Supply Chain Security Management Model in Cloud Computing

Dr.Mohd Nasrun Mohd Naw¹, Dr. Azham Hussain²

¹School of Technology Management & Logistics, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia.

²Professor & Chair, Human-Centered Computing Research Laboratory,
Universiti Utara Malaysia, Sintok, Kedah, Malaysia.

Article Info

Article history:

Received Apr 25, 2025

Revised May 18, 2025

Accepted Jun 05, 2025

Keywords:

Internet of Things (IoT)

Cloud computing

Supply chain security

Supply chain risk management

Cloud computing techniques

ABSTRACT

In today's business environment, the impact of information technology (IT) on the agility of supply chain management (SCM) systems is highly apparent. The business environment is impacted by competition pressure as well as ongoing disruptions such as new product and technology developments, declining products, and product proliferation. To gain a competitive advantage and succeed as a business, companies adjust to market shifts. This article combines effective cloud computing techniques with Internet of Things data networking technologies to develop supply chain management models. The development of supply chain security management models is also examined in this study from the viewpoints of participants, activity modes, and module operations. The data has been analyzed using these designs. The development of supply chain security management models from the viewpoints of participants, activity modes, and modular operations is investigated in this study in order to compare data. The model achieves a forecast accuracy of 98.48%, and its average test-running accuracy is approximately 89.60%, according to the testing findings. The total stability of the design across several builds is also around 96.02%, according to stability testing. According to research, the Internet of Things and cloud computing holds great promise for supply chain security management, potentially providing companies with better options in this field.

Corresponding Author:

Dr.Mohd Nasrun Mohd Naw,
School of Technology Management & Logistics,
Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia
Email: nasrun@uum.edu.my

1. INTRODUCTION

SCM, or supply chain security management, is the process of planning how products and services are distributed from vendors to consumers. It involves a complex network of procedures, including distribution, storage, transportation, and production. Companies that wish to remain competitive in today's globalized market, where supply chains may span many continents and countries, must efficiently manage their supply networks. SCM is responsible for ensuring that customers receive goods and services on time, in acceptable condition, and at a fair cost. To achieve this, manufacturers need to streamline their supply chain processes and collaborate closely with suppliers, logistics firms, and other relevant parties. Machine learning algorithms, artificial intelligence, and data analytics may help businesses understand how their supply chains work and make informed decisions. Furthermore, cloud-based solutions are increasingly often used to improve SCM's transparency, effectiveness, and agility [1].

Companies need to address supply chain security management and provide suitable security solutions to alleviate these concerns. These include putting in place a strong risk management strategy, bolstering infrastructure security, improving data privacy, and enforcing supplier background checks. To fully detect and reduce any risks, businesses must develop a supply chain security management model. Reducing safety hazards in manufacturing, sales, logistics, and other sectors requires a thorough evaluation of each supply chain link since they are interconnected [2]. Using techniques such as the Kraljic Asset Purchasing Model and methods centered on developing supply network security systems, regional collaborative growth, and fundamental technical breakthroughs, scholars have studied supply chain security management models. Organizational integration is made easier for businesses working in this context by supply chain management, or SCM. The supply chain is an intricate network of producers, distributors, retailers, warehouses, and supplies. It makes it possible to acquire, process, and transport raw resources to customers. Developing and managing operational systems efficiently is the main goal of modeling and analysis in order to increase competitiveness through the production of superior goods and services [3].

A supply chain security administration model based on cloud computing and the Internet of Things needs to be created and put into place in order to guarantee information security and improve the productivity of supply chains, flexibility, and open connection. Companies may gain a better understanding of how their supply networks work and make wise decisions by utilizing artificial intelligence, statistical analysis, and prediction algorithms. With the use of cloud-based technology, this strategy may effectively manage supply chain information security threats, standardize management of supply chain storage and analysis, and create a corresponding information security guarantee system. Additionally, it supports the industry's continuous growth and serves as a guide for businesses looking to develop a digital supply chain security management system [4]. Scholars who study security, operational procedures, and strategies highlight the influence of big data on supply chain security management. The expanding Internet of Things (IoT) also has the benefit of linking buildings, equipment, and networks from many sources. To create a supply chain security management system that permits ongoing tracking, data analysis, processing, and storage, cloud computing enables IoT devices to offer intelligent and useful services [5].

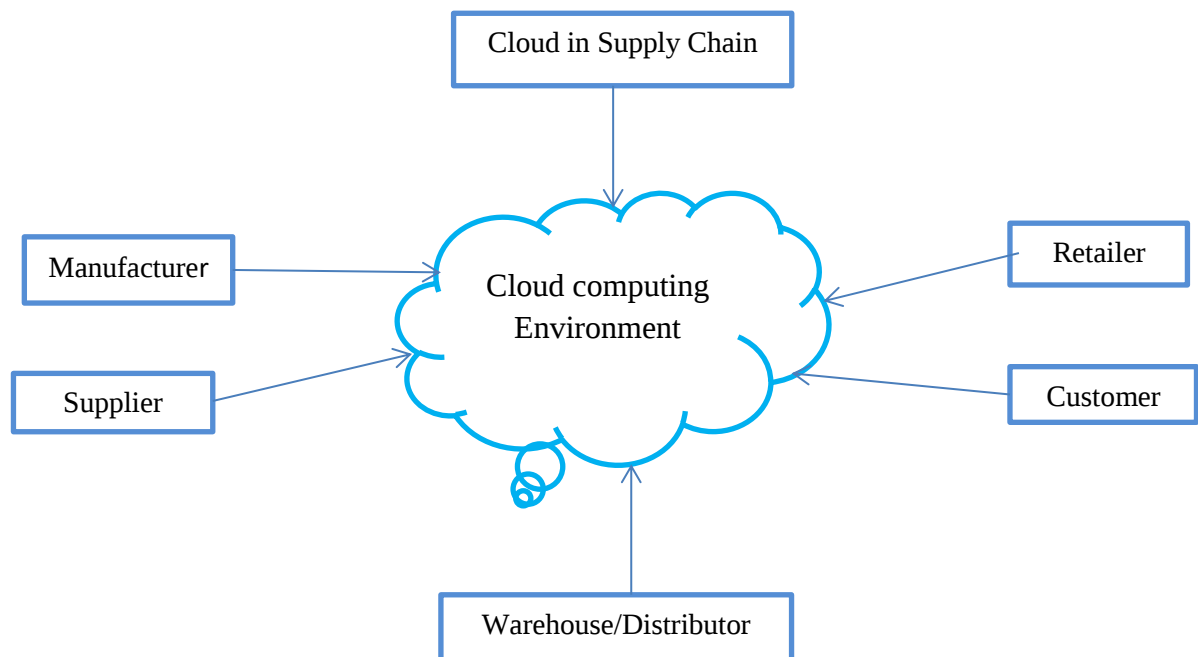


Figure 1. Cloud in supply chain networks environment

The cloud in a supply chain network environment is shown in Figure 1. Theoretically, applications for cloud computing in SCNs appear to be more affected by the hotly debated innovation diffusion concept. According to this article, using technology in a collaborative supply chain system requires trust. Due to their increased vulnerability to risks and opposition, SMEs are less inclined to adopt purportedly integrated cloud computing technologies [6]. However, due to their worldwide connectivity and service offerings, these cloud-based solutions are a godsend for multinational corporations.

Supply chain management recognizes innovation and new technology investment. According to The Worldwide Supply-Chain Forum, supply chain administration is "...the interconnectivity of key organizational processes from end users through the original vendors that provide services, goods, and data that add value" for customers and other partners. "Maximize profitability and earnings for the company as well as the whole supply chain network including the end customer" is the goal of supply chain management, as opposed to managers' limited emphasis and the adversarial relationships between suppliers, customers, and logistics providers. An integrated supply chain's primary advantage is that it allows for more accurate inventory reactions to changes in demand, which results in more appropriate stock levels across the supply chain [7]. Better information flow between supply system members produces more up-to-date information.

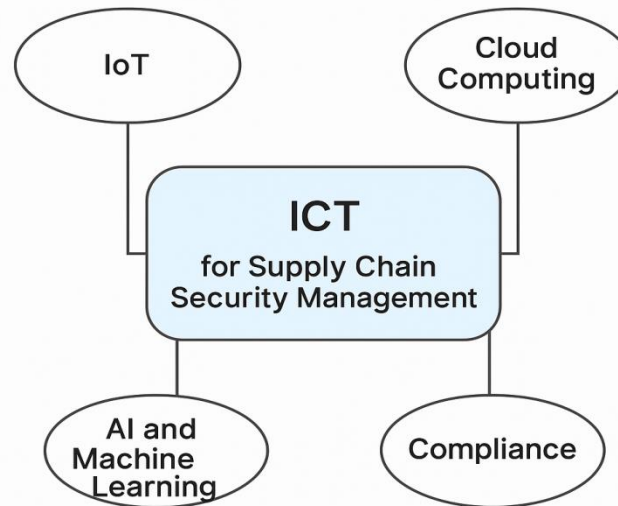


Figure 2. ICT Components in Supply Chain Security Management

Figure 2 illustrates the fundamental components of Information and Communication Technology (ICT) that contribute to effective Supply Chain Security Management. ICT integrates four major technologies:

- **Internet of Things (IoT):** Using sensors and smart devices, IoT makes it possible to track and collect data in real-time throughout the supply chain.
- **Cloud Computing:** Makes it easier to store and process data remotely and scalable, guaranteeing smooth data access and collaboration.
- **AI and Machine Learning:** It examines large data sets to find anomalies, improve sales practices, and predict risk.
- **Compliance:** Guarantees compliance policies, regulatory regimes, and security standards are followed in the supply chain and logistics network.

When bring these components together, you can create a robust, agile, and secured digital supply chain environment for improved risk management reliability and transparency. Additionally, global markets are transforming, and logistical operations have becoming increasingly complex, broadening their risk profile. Many believe that the new thinking on operational excellence must include a digital transformation and integration of smart technologies. As a result, businesses are now able to---access real-time data leveraging the latest cloud computing infrastructures, and gather data from sensors enabled by the Internet of Things capable of predictive maintenance, inventory adjustments, and flexible demand forecasts.

The essential capabilities identified above are vital to identify anomalies, reduce risks generated by a digital and real-world environment, and optimize operations. And of course, in regard to regulatory requirements, there are a variety of supply chain-specific compliance regimens, such as overall ICT compliance, GDPR, and ISO/IEC 27001, all of which have significant requirements for strong, transparent,

and secure ICT based models. Furthermore, cloud platforms combined with AI and machine learning, enable automation of threat detection and response systems. Consequently, putting in place an ICT-enabled supply chain security management model is both a strategic imperative and a proactive step toward intelligent and resilient supply networks.

2. LITERATURE REVIEW

Gonul Kochan et.al [8] introduced Understanding how supply chain resilience is impacted by cloud-based information and communication technologies. This research aims to investigate potential differences in supply chain operational performance and stability between cloud-based and traditional ICT (information and communications technology) systems. The recommended method shows that the relational antecedents of coordination and collaboration, rather than the kind of ICT platform, determine the resilience and effectiveness of the supply chain. This study quietly demonstrates that the ideas of cooperation and coordination enabled by ICT are forerunners of supply chains' adaptability and resilience. Additionally, research shows that supply chain resiliency acts as a mediator in the interactions between flexibility in supply chains, coordination, and collaboration.

Gammelgaard et.al [9] developed the Effect of Cloud Computing on Supply Chain Management in the Future. In the proposed method, digital technology is the main factor that makes supply chains (SCs) more competitive. CC capabilities provide responsiveness and architectural flexibility to competitive SC challenges. SC partners have the option to employ a CC-based Internet structure and a virtual environment for "data collaboration." The SC model transforms from a traditional, linear structure to an administrative model when all partners collaborate. Platform-based supply chain management, or SCM as it is now known, will represent a significant shift in the development of the industry. The study provides managers with information that they may utilize to comprehend and create the future generation of supply chain management (SCM) using CC, a contemporary and widely accessible ICT tool.

Al Mahmud et.al [10] proposed examining the use of RFID and IoT to increase supply chain management's efficiency and transparency. To enhance decision-making and operational efficiency, supply chain management, or SCM, is increasingly relying on technologies like RFID and the Internet of Things (IoT). These technologies allow data, information, products, and physical objects to be integrated across the supply chain by automating and optimizing business operations. In the proposed method, the goal of RFID-IoT, or the convergence of RFID and IoT, is to create seamless, highly secure automatic sensor systems. This connection enhances supply chain responsiveness and visibility by enabling real-time observation and tracking of items. A comprehensive analysis of current research indicates that RFID-IoT has the potential to significantly improve supply chain management (SCM) through cost reduction, productivity gains, and improved customer satisfaction.

Yesodha et.al [11] developed the Internet of Things (IoT)-Based Predictive Analytics and Automation in Supply Chain Management. The benefits of increased customer satisfaction, more economical supply chain processes, and improved supply chain management visibility might be achieved in the proposed work by leveraging IoT-based analytics and automation. Predictive analytics algorithms combined with automated structures can provide insights into supply chain operations, anticipate changes in client expectations, and help agencies properly plan and organize for the future. IoT may also be used to analyze supply chain practices, pinpoint areas for improvement, and stop potential disruptions.

Idowu et.al [12] introduced Issues with CyberSecurity in Cloud-Based ICT Systems. Cloud computing presents a wide range of CyberSecurity issues that jeopardize integrity, availability, and confidentiality as it develops to change the information and communication technologies (ICT) landscape. With a focus on critical vulnerabilities threat profiles, misconfigurations, data breaches, and inadequate identification and access limitations, this research provides a comprehensive analysis of the evolving threat environment in cloud-based ICT systems. The hazards posed by quantum computing, AI-driven attacks, and intricate multi-cloud settings are also examined. Modern strategies like DevSecOps, encryption techniques, Zero Trust Architecture, and threat detection driven by AI are also evaluated.

Toorajipour et.al [13] developed The Development of IoT Business Model Types and Their Effects on Supply Chain Administration. The servitization type moves the emphasis from commodities to service offerings to improve fundamental goods and operational flexibility, whereas the connectivity type concentrates on based on information monitoring and interactions between devices, users, and organizations. The data ecosystem type deals with collaboration and interdependence. The suggested approach offers data to businesses wishing to improve supply chain management and alter their company structures using IoT technology.

Temjanovski et.al [14] introduced cloud computing in supply chain and logistics management settings. A state-of-the-art technological solution, cloud computing enables companies or organizations to

host and operate their services without worrying about the dependability and security of information flow. Cloud computing makes it simple for businesses to adopt cutting-edge technologies like augmented reality, stability, security, advanced mobile apps, and potent analytics. Supply chain management and logistics are using them more and more. Because it saves money, time, and effort while building their IT infrastructure, cloud computing in supply chain management is very advantageous to logistics organizations. One important factor in this digital transition is cloud computing, which acts as a catalyst.

3. METHODOLOGY

To construct supply chain management models, the suggested approach in this research combines efficient cloud computing methodologies with Internet of Things data connecting technologies. In this study, we also examine the development of security for supply chain approaches from the viewpoints of module operations, activity modes, and participants. We then use these frameworks to compare data. According to research, supply chain safety administration benefits greatly from cloud computing and the Internet of Things; this might provide businesses with access to more potent supply chain security management solutions.

3.1 Cloud Computing

A new technology called cloud computing can be used anywhere in the world at any time with an internet connection. It is a strategy for data outsourcing that aims to manage concerns and data storage. Implementing cloud computing has several advantages, including lower infrastructure costs, increased performance, flexibility, ease of use, and cost savings. Private, publicly available, connected, and combination are the other four categories of cloud computing delivery (deployment) strategies. As a result, cloud computing types were separated into three groups: Software as a Service (SaaS), which includes Google applications such as Gmail, and Papers; Technology as a Service (IaaS), which includes Salesforce and Amazon web services; and Platform as a Service (PaaS), which includes IBM and the online retailer's EC2 offerings [15]. The architectural cloud system will be suggested in the next part.

3.2 CCIS, or Cloud Computing Information System, for Supply Chain Information

Cloud computing technology uses central, distant servers such as software servers and servers that store databases, as well as the internet, to send and retrieve data and different applications. Alongside supply chain management, other technologies may be utilized, including processors, data center, cloud computing, logistics management, and handheld gadgets (such as smartphones and tablets). The supply chain management structure utilizing cloud computing is depicted in Figure 1 [16].

Figure 3 illustrates how data from the supply chain phases will be sent to the server for databases and software servers before being received by the information system server device (IS server engine). The construction of the Cloud Computing Information System (CCIS) consists of the following four primary components:

The Mobile Client: Portable gadgets such as smartphones and tablets are examples of smart mobile devices that may send data and information to the knowledge system server engine during supply chain stages via a cloud service. Additionally, cloud computing will provide the mobile client with information on supply chain phases;

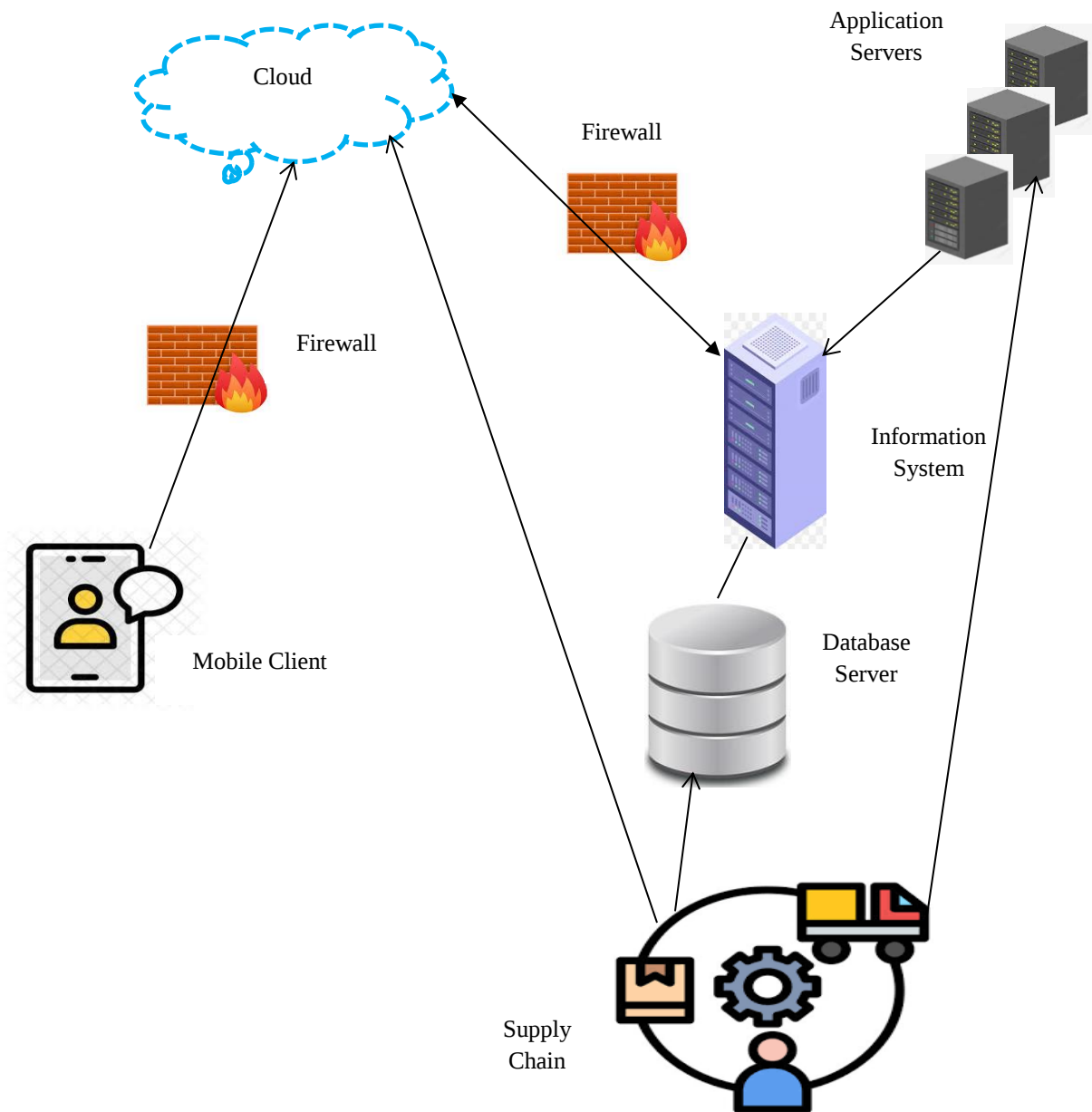


Figure 3. Supply Chain Management's suggested Cloud Computing Information System (CCIS)

The Firewall: Two firewalls—one between the cloud service and the Information server engine, and another between the cloud and the phone or tablet client—have been investigated. Firewalls will safeguard the data being communicated and delivered to the devices along the precast supply chain processes.

IS Server Engine: During the supply system stages, the IS server engine will process the data provided by the information storage server, application servers, and mobile clients; and

The Cloud Server: Information generated by the IS client engine will be sent to the cloud with firewall authority. During the supply chain phases, the mobile client will also receive the information via the cloud.

3.3 Security concerns on supply chain and cloud computing

Investigations are conducted on the potential integration of CC technology in SCM to boost efficiency and save expenses. The authors also explore the benefits of CC, such as increased flexibility and accessibility, and present a case study of a cloud-based supply chain management system utilized in manufacturing industries. It looked at the applications of CC in supply chain management, namely in the

areas of inventory control, processing orders, and logistics. They give an example of a cloud-based supply chain management system that has been used at a Chinese logistics business and go over the advantages of these systems, such as real-time data sharing and collaboration. The primary focus of the study on the relationship between CC and SCM is on the areas of creativity, effectiveness, and agility. These studies demonstrate the increasing awareness of CC and its possible benefits for SCM. Utilizing cloud-based technology may provide businesses with a competitive edge and increase supply chain efficiency. A thorough analysis of the potential challenges and best practices associated with cloud adoption is essential to ensuring effective installation and management [17].

3.4 Better supply chain and cloud computing disaster recovery

Studies have examined the possibility of using CC to enhance disaster recovery in SCM. It investigates how CC could enhance SCM's disaster recovery. The authors discuss the benefits of cloud-based disaster recovery systems, such as their increased flexibility and scalability, and provide recommendations for implementing these solutions. Data backup and recovery, in particular, looks at how CC might enhance disaster recovery in SCM. They go over the advantages of cloud-based disaster recovery systems, such as shorter recovery times and less downtime, and offer suggestions for putting these solutions into practice. The advantages of adopting cloud-based systems for disaster recovery, including shorter recovery times and less downtime are covered, and suggestions for utilizing cloud-based recovery services are provided. They concentrate on data backup and recovery while researching how CC could enhance SCM disaster recovery.

3.5 Cloud computing and supply chain reliance on Internet connectivity

The impacts of internet connectivity on SCM with CC are investigated in the research that follows. In addition to examining how CC may improve SCM, they emphasize how important internet connectivity is for cloud-based systems. According to the authors, cloud-based supply chain solutions may not function as well if data transfers are irregular or slow due to poor internet access to look at the potential effects of CC on the operational and security elements of SCM. They emphasize that cloud-based systems will not function properly without continuous internet access and suggest implementing redundancy mechanisms to protect against any internet connectivity interruptions. They note in their examination of a case study on the application of CC in SCM that the implementation's success depended on reliable internet access. The authors recommend setting up backup plans and considering the possible impacts of internet connectivity difficulties in order to preserve company continuity. According to this research, reliable internet connectivity is crucial for cloud-based supply chain management systems [18]. CC might help SCM, but if internet access fails, system performance might deteriorate. Businesses should thoroughly examine the potential challenges and best practices associated with internet connection for cloud-based SCM to achieve successful deployment and administration. System performance may suffer if internet access is not available, even though CC might aid SCM. For a cloud-based supply chain to be deployed and administered successfully, businesses should carefully consider the possible issues and guidelines related to internet connectivity.

3.6 Decreased investment in cloud computing and supply chain

According to some research, adopting CC may result in decreased SCM capital expenditures. It draws attention to the possibility of lower initial expenses when using cloud-based supply chain management (SCM) systems. According to the authors, businesses may save a fortune by utilizing CC to free up money for other costs like pricey software and equipment. The literature on CC's influence on SCM is surveyed. They point out that using cloud-based systems can save organizations a significant amount of money by removing the need for them to make significant investments in software and IT infrastructure. Studied CC's capacity to improve SCM agility. Because cloud-based systems eliminate the need for enterprises to invest in expensive IT infrastructure, the authors note that users can save money. These studies demonstrate how CC may reduce the capital costs associated with SCM. Using cloud-based solutions rather than costly IT gear and software can result in considerable cost savings for businesses [19]. Thoroughly weighing the possible costs and benefits of cloud adoption is necessary for ensuring that it is a cost-effective solution for the particular needs of the business.

4. EXPERIMENTAL RESULT AND ANALYSIS

The security of supply chain management involves a big task that is necessary to safeguard the interests of customers and enterprises. Putting in place a thorough testing indication system is essential to accurately evaluating, monitoring, and improving supply chain security. Cloud-based and Internet of Things-based supply chain security management architecture is developed to meet this need by guaranteeing the safe movement of goods and data across the supply chain. According to this paradigm, the security chain

management platform acts as the focal point of the system, around which other elements are grouped. Potential applications for cloud computing and the Internet of Things include integrating security chain systems and enhancing their performance. The following elements need to be considered when confirming the model.

Table 1. Proportion of various supplier types

Supplier type	Element Rate	Cost Rate	Yield Rate	Response Rate
Manufacturer	17	35	25	25
Distributor	25	35	25	30
Supplier	30	25	25	20
Partner	43	20	40	45

Tools for communication to pool resources and break down barriers. This is another important objective of developing a supply chain security management approach. The partners' risk trend is the shortest of the four groups formed from the overall supplier categories in Table 1. The supply and demand sides of a well-established logistic system, with commensurate power foundations, use efficient information, share operational hazards in supply chain security management, and come to favorable long-term agreements.

Table 2. Evaluation indicators' judgment matrix

	a1	a2	a3	a4
a1	2	5	2	1/2
a2	1	2	2	5
a3	1/2	1	1/3	1/3
a4	2	1/4	4	1

The information in Table 2 demonstrated the interactions between the different supply chain system components as the supply chain security management strategy was being established. The effect elements in the database are created and statistically assessed using cloud computing.

4.1 Supply Chain Security Management Model Implementation

For basis evaluation indicators, the experimental model is constructed. The original data is primarily simulated in this experimental model, and algorithms are used to match and replicate operations on the replica data. Iterative stability testing of several operations and the precision of supply chain stability trend forecast are the primary tests in the supply chain security management system. Table 3 shows the accuracy values of stable supply chain trend.

Table 3. Stable supply chain trend accuracy

	Manufacturer	Distributor	Supplier	Partner	Average
Effectiveness	92.65	91.87	94.44	96.32	99.43
Performance	89.19	90.18	96.54	95.23	97.67
Budget	90.12	89.90	93.23	95.99	97.01
Test	88.76	89.21	92.32	94.76	98.12
Abnormal	87.10	88.47	90.17	92.48	95.44

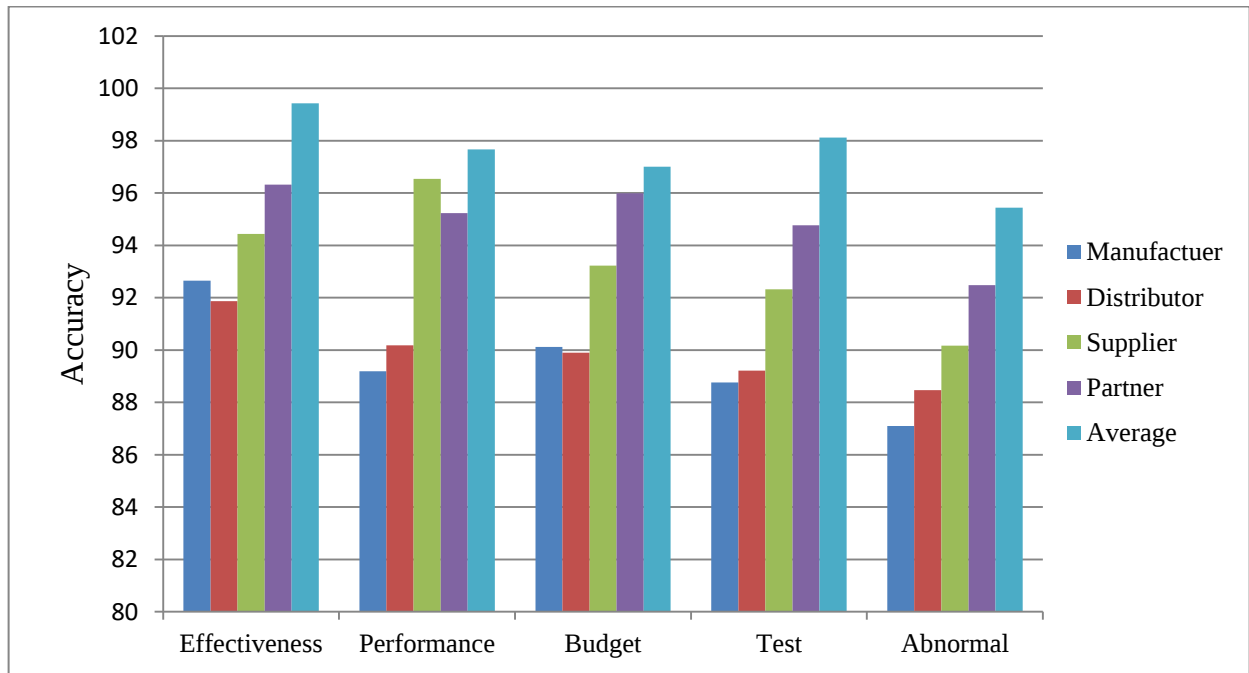


Figure 4. Accuracy of forecasting steady supply chain patterns

Figure 4 shows that while the subject objects in the production chain are distinct, the data feedback influences on model assessment and examples are also diverse. The steady trend projection's overall average accuracy, even with considerable fluctuation among the many components, is around 90.60 percent. For example, most partners' assessment indicators have a basic value of more than 92%, which is higher than what distributors, vendors, and manufacturers have. As such, participants are important nodes in the supply chain network, and a variety of factors, such as prior partnerships and contractual agreements, impact their inclination for risk factors. These factors collectively establish the partners' primary responsibility for supply chain security oversight. Up to 99.43% of gain projections prove to be correct.

Models for logistics security management are evaluated by manufacturers with very low-performance values; trend forecast accuracy is roughly between 80% and 90%. This implies that a variety of supply chain management procedures affect makers, who serve as middlemen between suppliers and resellers. Consequently, supply chain security management models' steady trend estimates for manufacturing are incredibly inaccurate. The reduction of unsolved trends in supply chain security administration requires the use of the technical framework of supply chain nodes, which are represented by production; in conjunction with the advantages of cloud computing and the multi-party communication capabilities of the Internet of Things. The result will be efficient and rapid communication of information.

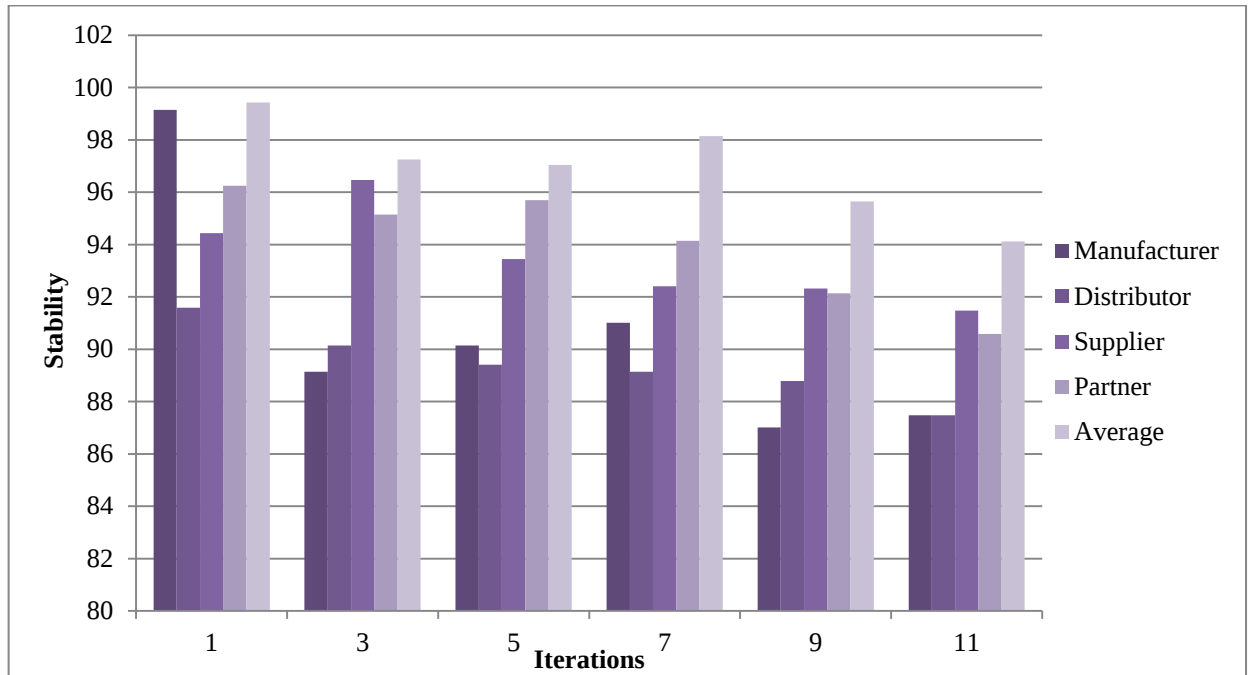


Figure 5. Stability testing of model iteration

Multiple stability testing rounds can be used to examine the scenarios that different supply chain node entities encounter in order to determine the operational reliability trend of the supply chain security management model. Figure 5 shows that, over several rounds, the total operation's average stability level is around 96.02%. The stability of the producer fluctuates the greatest, fluctuating by around 4 %, while the other nodes usually fluctuate by roughly 3%.

Additionally, the judgment matrix and evaluation indicators provide insightful information about the influences of various performance metrics on overall system stability. By organizing these indicators into a weighted framework, the model makes sure that decisions are made with consideration for several operational dimensions rather than just one. This method balances cost yield responsiveness and risk to improve the resilience of security management.

The combination of original and replicated data facilitates the modelling of real world conditions in simulation-based experimentation. The modelling technique can represent a dynamic, changing situation of supply and demand, as illustrated by stability in the aggregate across repeated iterations. Cloud and IoT integration not only allows for the provision of static risk protection but also promotes a dynamic learning-based model that can respond to changes in supply chain operations.

To get initial real-world data and determine the supply chain security administration model's basic efficacy while in use, it is feasible to assess its correctness and stability. The design may be examined from a variety of angles, including user testing, which assesses the model's viability and efficacy by looking at it from the viewpoint of certain users. Among the tests that address the model's essential features in response to client demands are practical and usability evaluations. The goal of security testing is to determine if the template is vulnerable to manipulation or malevolent assaults. Testing the supply chain security administration model for protection adaptability, dependability, and other aspects guarantees its effectiveness and security.

5. CONCLUSION

The use of information and communication technologies to safeguard distribution networks has increased as a result of the Internet of Things and cloud computing. It is essential to do research on developing an ICT supply chain safety management model based on online technologies and the Internet of Things. This essay also examines the development of supply chain security management models from the viewpoints of participants, activity modes, and module activities. These models are then used for data comparisons. This study examines the construction of supply chain security management models by analyzing data from the perspectives of participants, activity modes, and modular operations. The experimental findings indicate that the model's average accuracy in running tests is around 89.60%, and its

advantages in forecast accuracy may reach 98.48%. Additionally, stability evaluation reveals that the model's average stability across multiple versions is around 96.02%. Along with comparing and analyzing the benefits of cloud computing and the Internet of Things, this article also discusses common supply chain information security challenges using a number of relevant security management techniques and tactics. In addition to managing cloud computing and Internet of Things security, this strategy may be utilized to increase the competitiveness and information security level of the business information communication supply chain.

Practical Implications

Using this model can be advantageous for sectors like manufacturing, retail and logistics. By achieving real-time tracking and coordination, logistics providers can lower theft and delays. Retailers can use data-driven planning to improve customer service and inventory visibility while manufacturers can improve vendor coordination and secure production workflows. IoT devices offer real-time data from all over the network while cloud platforms guarantee scalability and centralized control. When combined, they allow for a more robust and interconnected supply chain system that can react quickly to interruptions.

Future Scope

Blockchain integration may be included in future projects to ensure increased transaction, transparency and traceability in supply chain. The use of AI and machine learning can also support increased predictive analytics, having real-time, data-driven, automatic responses to potential risks or cosuch as shortages, delays or security breaches.

Limitations

While the model may be valuable, its implementation in regions with insufficient infrastructure may be limited by requiring stable internet connectivity. Risk factors are also present in cyber-security and data privacy regards for cloud-based and Internet of Things enabled systems. Finally, very small to medium-sized organisations (VMOs and SMEs) may struggle with cost and technical complexities which indicate that more accessible modular possibilities are needed in further works.

REFERENCES

- [1] Yenugula, M., Sahoo, S., & Goswami, S. (2023). Cloud computing in supply chain management: Exploring the relationship. *Management Science Letters*, 13(3), 193-210.
- [2] Matthew, U. O., Kazaure, J. S., & Okafor, N. U. (2021). Contemporary development in E-Learning education, cloud computing technology & internet of things. *EAI Endorsed Trans. Cloud Syst.*, 7(20), e3.
- [3] Islam, R., Ansari, M. E., Dewan, M. A., Sultana, S., & Rivin, M. A. H. (2024). Supply Chain Management Analysis and Design for a Variety of Economic Scenarios, Including Data and System Administration. *Journal of Software Engineering and Applications*, 17(10), 770-785.
- [4] Wang, C., & Zhang, H. (2023). Construction of a Supply Chain Security Management Model for Information and Communication Technology Based on the Internet of Things and Cloud Computing. *Procedia Computer Science*, 228, 745-754.
- [5] Shambulingappa, H. S., & Rashmi, T. V. (2023). Impact of IoT and Cloud Computing on Enterprise Supply Chain Security Management. *International Journal of Advanced Scientific Innovation*, 5(8).
- [6] Sundarakani, B., Kamran, R., Maheshwari, P., & Jain, V. (2021). Designing a hybrid cloud for a supply chain network of Industry 4.0: a theoretical framework. *Benchmarking: An International Journal*, 28(5), 1524-1542.
- [7] Amini, M., & Jahanbakhsh Javid, N. (2023). A multi-perspective framework established on the diffusion of innovation (DOI) theory and technology, organization, and environment (TOE) framework toward supply chain management system based on cloud computing technology for small and medium enterprises. *Organization and Environment (TOE) Framework Toward Supply Chain Management System Based on Cloud Computing Technology for Small and Medium Enterprises (January 2023). International Journal of Information Technology and Innovation Adoption*, 11, 1217-1234.
- [8] Gonul Kochan, C., Nowicki, D., & Glassburner, A. (2024). Understanding the influence of cloud-based information and communication technology on supply chain resilience. *Benchmarking: An International Journal*.
- [9] Gammelgaard, B., & Nowicka, K. (2024). Next generation supply chain management: the impact of cloud computing. *Journal of Enterprise Information Management*, 37(4), 1140-1160.
- [10] Al Mahmud, M. A., Hossan, M. Z., Tiwari, A., Khatoon, R., Sharmin, S., Hossain, M. S., & Ferdousmou, J. (2025). Reviewing the Integration of RFID and IoT in Supply Chain Management: Enhancing Efficiency and Visibility. *Journal of Posthumanism*, 5(3), 409-437.

-
- [11] Yesodha, K. K. R. K., Rajendran, P., Bhalerao, M., Gupta, K., & Yuvaraj, N. (2025, February). Predictive Analytics and Automation in Supply Chain Management with Internet of Things (IoT). In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 01-05). IEEE.
 - [12] Idowu, E. (2025). Cybersecurity Challenges in Cloud-Based ICT Systems.
 - [13] Toorajipour, R. (2025). The Progression of Iot Business Model Types: Implications for Supply Chain Management. In The 58th Hawaii International Conference on System Sciences. HICSS 2025 (pp. 4139-4148). Hawaii International Conference on System Sciences (HICSS).
 - [14] Temjanovski, R., Bezovski, Z., & Apasieva, T. J. (2021). Cloud computing in logistic and Supply Chain Management environment. *Journal of Economics* (1857-9973), 6(1).
 - [15] Abedi, M., Rawai, N., Fathi, M. S., & Bin Mirasa, A. K. (2015). Cloud computing information system architecture for precast supply chain management. *Applied Mechanics and Materials*, 773, 818-822.
 - [16] Mahesh S.Aphale. (2022). Collabroration Complexity Reducing Strategy In Cloud Computing. *IIRJET*, 2(4).
 - [17] Jiang, W. (2019). An intelligent supply chain information collaboration model based on the Internet of Things and big data. *IEEE Access*, 7, 58324-58335.
 - [18] Dr. Yassir. S.K. Osman, Dr. A. Rajalingam, & Dr. Jayakumar. M.S. (2023). A Novel Application Service Security Using Peer-to-Peer Trust Slicing Trust Model. *IIRJET*, 8(3).
 - [19] C.Ashwini, J.Muthu, B.Karthikeyan, & V.Vinith Raj. (2022). An Efficient Auditing Technique for Secure Cloud Computing Using Asymmetric Cryptographic Algorithm. *IIRJET*, 1(1).