ISSN 2581 – 3781

AJCSE ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info

Asian Journal of Computer Science Engineering 2025;10(2):1-11

REVIEW ARTICLE

Cybersecurity in Supply Chain Management Role of Identity and Access Management, Zero Trust, and Blockchain

Sreenivasulu Gajula*

Independent Researcher

Received on: 25-04-2025; Revised on: 16-05-2025; Accepted on: 28-06-2025

ABSTRACT

Supply chain management (SCM) has experienced a substantial digital revolution in today's digitally interconnected world, making cybersecurity a top priority. Supply chains are at a greater risk of cyberattacks that might interfere with procedures and compromise private information as they depend more on technological innovations. This paper explores the evolving cybersecurity landscape in SCM, emphasizing the critical need for robust security measures amid increasing digital integration. It examines key cybersecurity challenges, such as data breaches, ransomware, and third-party vulnerabilities, highlighting the robustness of the supply chain. Zero trust architecture, identity and access management, and other sophisticated security frameworks are the main topics of the research and blockchain technology, detailing their roles in enhancing protection, access control, and transparency across complex supply networks. Through real-world case studies from leading organizations such as IBM, Coca-Cola, Walmart, and FedEx, the paper demonstrates practical implementations and benefits of these technologies in securing SCM operations in additive manufacturing. The findings underscore the importance of adopting comprehensive, adaptive cybersecurity strategies to safeguard global supply chains against emerging threats and ensure operational continuity.

Key words: Blockchain technology, cyber threats, cybersecurity frameworks, cybersecurity, digital supply chains, supply chain management

INTRODUCTION

In today's digital-first economy, supply chains are no longer confined to the movement of goods – they represent interconnected networks of data, services, and financial flows that span global boundaries.[1] As organizations embrace innovations including cloud-based platforms, 5G, and the Internet of Things (IoT) to improve supply chain effectiveness, they simultaneously increase their exposure to cyber threats. The expanding digital footprint of modern supply chain management (SCM) has made cybersecurity not just an operational requirement but a strategic priority.

Recent cyberattacks such as the SolarWinds and Colonial Pipeline incidents have demonstrated the devastating impact of supply chain breaches on critical infrastructure, national security, and business continuity.[2,3] Threats range from ransomware and data theft to manipulation of IoT sensors and disruption of logistics networks. These challenges demand a fundamental abandonment of conventional perimeter-based fortification in favor of more dynamic, resilient security architectures capable of protecting against sophisticated and persistent adversaries.

To address this evolving threat landscape, cybersecurity strategies within SCM are increasingly shaped by three transformative technologies: Zero trust architecture (ZTA), identity and access management (IAM), and blockchain (BC).[4] IAM enforces user authentication and access safeguards, guaranteeing that critical systems can only be accessed by those who are authorized. ZTA continually checks each access request to remove assumed trust, regardless of origin. Blockchain, with its decentralized and immutable ledger, enhances transparency, traceability, and auditability across supply chain transactions.[5,6] This review explores how these technologies, individually and collectively,

Address for correspondence:
Sreenivasulu Gajula
E-mail: sreenivasgajulausa@ieee.org

contribute to building secure, trustworthy, and future-ready supply chains.

Objectives of the Paper

This work aims to explore the main cybersecurity issues that SCM systems must deal with and assess the effectiveness of using IAM, ZTA, and BC as ways to solve them. The study seeks to examine actual case studies to showcase best methods and suggest ways to improve the cybersecurity resistance of today's connected and digital global supply chains. As follows are the main insights from the study:

- Provides a detailed look at the cyber risks that are unique to digital supply chain environments
- Focuses on how IAM, ZTA, and BC support the safety and success of supply chain activities
- Offers valuable advice with detailed stories from top global organization cases
- Helps policymakers and industry experts set better strategies for cybersecurity protection in the supply chain.

Structure of the Paper

The following sections outline this document. Section II looks at the condition of SCM cybersecurity. Section III focuses on IDAM in SCM practices. Section IV of the report explores ZTA in supply chain settings. Section V looks at how BC technology is changing SCM methods. Case studies relating to supply chain cybersecurity are covered in Section VI. In the last section, the paper offers ideas for further studies.

CYBERSECURITY LANDSCAPE IN SCM

This is due to the digital upgrade of SCM, there is now a stronger link between suppliers, the logistics sector, and enterprise tools worldwide. Cybersecurity threats facing digitized supply chains are numerous, so it is important to fully understand their vulnerabilities and risks, as shown in Figure 1.[7,8] Strong cybersecurity is now vital for businesses to remain robust, constant, and trustworthy in the supply chain.

Figure 1 illustrates key cybersecurity layers within a supply chain system, including endpoints, data flows, identity controls, and access verification. It highlights the integration of technologies such as IAM, ZTA, and BC across procurement, production, distribution, and logistics networks.

Among cyber threats in sustainable supply chains, there is a possibility of data breaches, losing money, taking a hit to reputation, and disruptions to activities. The risks cover activities inside the organization and with outside suppliers, so a complete security approach is required.

Cybersecurity Challenges in SCM

At present, integrating cybersecurity measures is one of the main worries in sustainable SCM, so understanding what cybersecurity involves is very important.[9] Figure 2 shows the most frequent

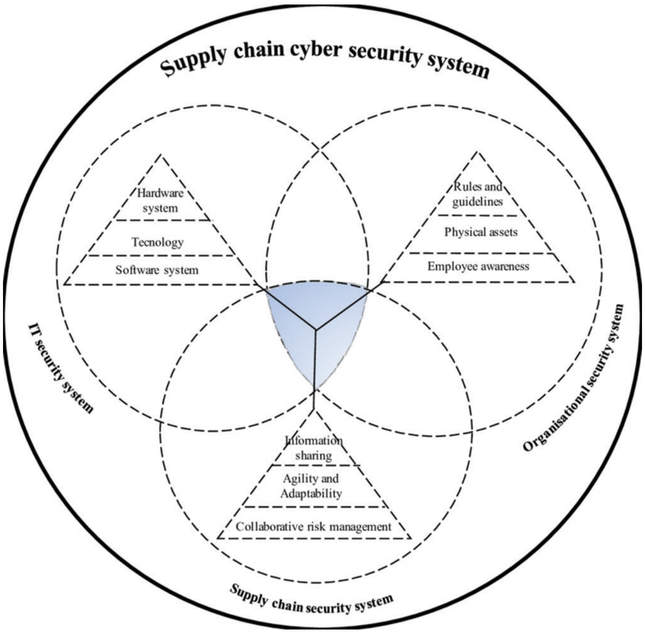

Figure 1: Integrated cybersecurity in supply chain management

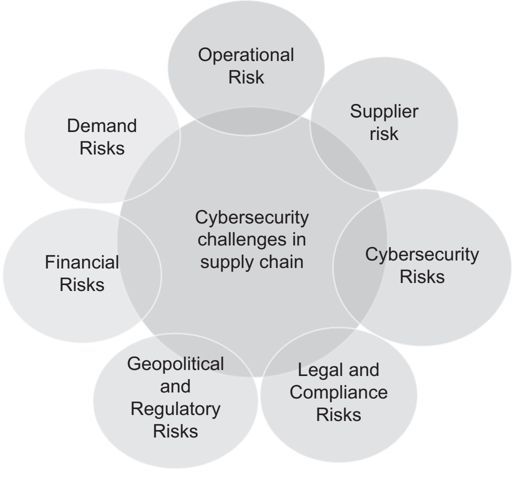
Operational Risk
Supplier risk
Demand Risks
Cybersecurity challenges in supply chain
Financial Risks
Cybersecurity Risks
Geopolitical and Regulatory Risks
Legal and Compliance Risks

Figure 2: Common cybersecurity risk categories in supply chain management

supply chain risk management (SCRM) risk factors, which are summarized in the following section:

- Problems in the supply chain, such as those in manufacturing, transportation, inventory management, or logistics, are types of hazards that might occur during normal processes. Machine failures, strikes by workers, traffic problems, shortage in supplies, frequent stops in production, and similar happenings can cause harm to the business.
- The performance or interruptions of suppliers in the supply chain are the root cause of these risks.[10] Company insolvency, unstable finances, poor-quality goods, late supply, and failing to obey regulations are hazards you may encounter with suppliers.

This visual representation of Figure 2 categorizes risk domains operational, supplier-based, demand-driven, financial, geopolitical, and legal while mapping potential impacts on confidentiality, integrity, and availability across the supply chain.

The Primary Challenges Include

- Operational risks: Issues in manufacturing, logistics, transportation, or inventory management, such as equipment failure, labor strikes, and supply shortages, can cause process bottlenecks and vulnerabilities in automated systems.
- Supplier-related risks: Rooted in third-party vulnerabilities, these risks include poor supplier cybersecurity posture, delayed deliveries, insolvency, and non-compliance with cyber standards. These risks become critical in highly connected supply chains lacking unified standards.
- Demand variability risks: Market fluctuations influenced by consumer preferences, seasonality, and economic shifts create unpredictability. Insecure customer data flows and inaccurate forecasting models may expose systems to fraud or manipulation.
- Financial risks: Arise from currency volatility, mortgage rate changes, or tightening credit conditions. These can impair the financial stability of supply chain partners and affect investment in cybersecurity infrastructure.[11]
- Geopolitical and regulatory risks: Emerge from trade wars, sanctions, political instability, and compliance mandates. These disruptions may force companies to adapt or restructure supply chains, often under insecure or unstable digital platforms.
- Legal and compliance risks: Involve IP protection, contract enforcement, and evolving regulatory landscapes. Cyber incidents impacting legal documentation, partner trust, or auditability can have cascading effects on operations and reputations.

Cybersecurity in Digital SCM

E-supply chains or digital SCM refer to an integration of digital technologies within SCM, facilitating the electronic exchange of capital, goods, and details among different stakeholders. The activities of supply chains are made more efficient with the use of digital technology, which is transparent and responsive. Cybersecurity means protecting computer and network systems as well as private information in digital SCM. Because so much technology is involved in supply chains today, strong cybersecurity steps are crucial for any business. Large cybersecurity issues faced by e-supply chains include data breaches, ransomware, and security weaknesses from third parties, phishing, and attacks on software supply chains.[12] It is important to have strict cybersecurity measures in place because these attacks could let out confidential data, pause operations, and seriously damage the company's finances and reputation. Major cybersecurity threats in e-supply chains are as follows:

- Data breaches: When sensitive data are accessed without permission, it can cause major financial and operational problems and threaten a company's ability to follow the rules and keep working.
- Ransomware attacks: Attackers sometimes encrypt major data and hold it hostage until a ransom is paid, which can heavily disrupt how the supply chain operates.
- Phishing and social engineering: The goal of these strategies is to acquire unauthorized access to systems by taking advantage of human behavior, most often by sending misleading emails or messages that fool workers into giving important information.

Key Concepts of Cyber Security Based on Supply Chain

Here are the main key concepts of cybersecurity-based SCMs:

- Data protection: Data protection in supply chain cybersecurity means preventing unauthorized people from accessing supplier info,[13] transaction details, and stocks. This is made possible by strong encryption tools, strict access permissions, and secure storage areas kept throughout the supply chain.
- Threat detection and response: Advanced tools are put in place by organizations to watch over their supply chain operations in real time. Such systems quickly spot cyber threats, including malware, phishing attacks, and attempts to enter unauthorized systems, which results in fast actions by supply chain members to secure their operations.
- IAM: IAM frameworks are used by supply chains to impose role-based access to vital data and systems. Access to some digital assets is controlled by special techniques such as ICAM and MFA.
- SCRM: Properly assessing cybersecurity risks from suppliers and logistics partners is truly important in managing the safety of a supply chain. When doing this, people need to confirm that suppliers are meeting the security standards set by their business and also check their cybersecurity strengths.
- Endpoint security: From corporate servers to IoT tools in logistics, all endpoints should be defended by firewalls, antivirus, and EDR tools in order to stop criminals from attacking.
- Network segmentation: Supply chain network segregation reduces the possibility of lateral cyber threat movement. Consequently, the whole supply chain system is not at risk if one part is compromised.

Impacts of Cybersecurity Measures in Supply Chains

Cybersecurity within supply chains is now a top concern for organizations globally. As technology makes our supply chains more digital and linked, the chance that cyber threats will negatively affect our efficiency, finances, and image has grown. Federal agencies may evaluate the possible effects of cybersecurity incidents on their supply chains via the creation and use of the C-SCRM Interdependency Tool.[14] An important step forward in the sector, this technology provides a workable answer for businesses worried about cyber supply chain threats and how to analyze and lessen their interconnected risks. The C-SCRM tool’s ability to model complex operational environments and the supplier chain. Information security across the whole supply chain was introduced with evaluation and certification, together with the proposal of an appropriate metrics framework for assessing cybersecurity controls. Experts have shown the importance of adopting IEC 62443 in industry and of frequently checking safety measures.

ROLE OF IAM IN SCM

Through the IAM framework, authorization, privilege management, and authentication of users are managed in cloud environments.[15,16] If access to the cloud is managed properly, it will help avoid credential theft, illegitimate access, and misuse of privileges. IAM is a fundamental part of Zero Confidence Security. This form of security is always a check for identification before giving access and assumes no one, system, or network can be trusted implicitly.

IAM is vital for protecting supply chains, particularly when it comes to systems and services hosted on the cloud.[17] Data integrity and security in supply chains rely on having strong access control over the many individuals, organizations, and technologies involved. IAM ensures the responsible handling of vital supply chain resources, which cuts down the risk of unauthorized access.

Several Critical Components of IAM

Here are some critical components of IAM as follows:

- User authentication: Verifies the identity of users using methods such as passwords, biometrics, security tokens, and MFA
- Access control policies: Determine user permissions using models such as role-based access control, attribute-based access control, and privileged access management

- Identity federation: With federated identity management systems, you may access several cloud services with a single set of credentials[18]
- Continuous monitoring and audit trails: Keeps tabs on user actions, patterns of access, and irregularities to spot suspicious conduct and possible security breaches
- Identity lifecycle management: Automated account provisioning, account updates, and account deactivation to cut down on identity sprawl and misuse of access.

The Role of IAM in Strengthening Cloud Security

IAM is essential to contemporary cybersecurity because it addresses changing threats and enforces strict access control policies across cloud environments. Figure 3 shows the role of IAM, which is given below:

Traditional access control mechanisms often fail to prevent identity-based attacks, as follows:

- Credential theft and phishing attacks: Hackers get unauthorized access to cloud resources by stealing login credentials using social engineering tactics[19]
- Privilege escalation attacks: Malicious actors exploit weak access controls to elevate their privileges and compromise sensitive data
- Insider threats: Legitimately authorized partners, independent contractors, or employees may abuse their rights for nefarious or careless purposes
- Session hijacking: Attackers intercept or steal active session tokens to gain control of cloud-based applications and services.

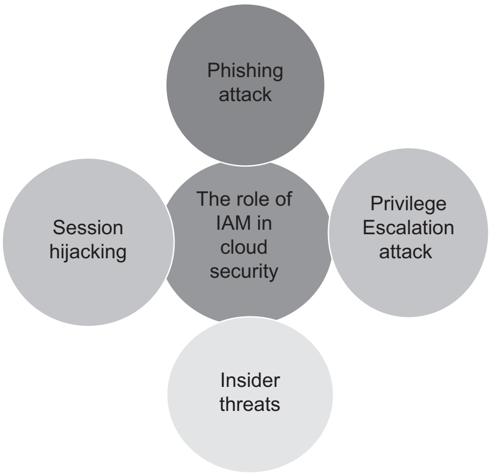
Phishing attack
Session hijacking
The role of IAM in cloud security
Privilege Escalation attack
Insider threats

Figure 3: Role of identity and access management in security

ZTA FOR SUPPLY CHAINS

NIST provides the following operational definitions of zero trust and ZTA. The "Strafes" system design aims to use the "zero trust" concept, which aim to simplify the process of making precise access decisions for each request by simulating a hacking attack on the network.[20] Figure 4 shows a simplified version of zero trust access that is used to regulate access for each and every connection request, using policy decision/enforcement points (PDP/PEP) with the goal of illustrating the interplay between authentication.

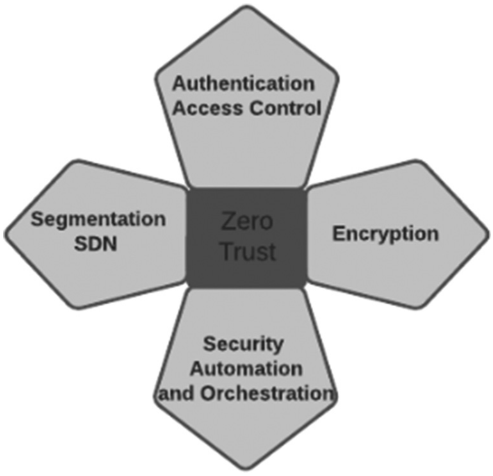
Authentication Access Control
Segmentation SDN
Zero Trust
Encryption
Security Automation and Orchestration

Figure 4: Zero trust in supply chain management

The "zero trust" paradigm in cybersecurity is centered on protecting resources and the notion that trust should never be given tacitly but rather has to be continuously assessed. Figure 4 shows the zero-trust paradigm, which defaults to not trusting any process, whether it is within or outside the network. A movement in emphasis from networks, network devices, and perimeters to data and enterprise resources is at the heart of zero trust, also known as perimeterless security. Under this model, any organization wishing to access these resources is required to validate its identity.[21] There are companies who build zero-trust platforms and vendors that apply zero-trust ideas to their current security offerings. The developers of a zero-trust platform, among them ColorTokens, detail how their product protects against advanced persistent attacks. Several companies have been working on documentation to tell the general public about ZTA and how their products work with the architecture. There are several components as follows:

- Communication security: Communication remains secure regardless of the user's location, ensuring data integrity and confidentiality.
- Session security: The resource each session has access to is different. Authentication and authorization processes are resource-specific and cannot be reused across sessions.
- Access control: Dynamic policies govern resource access based on observable client identity, application state, and asset state.
- Minimum-security posture: Enterprises maintain continuous monitoring of all owned and connected devices to ensure a secure baseline across all assets.
- Continuous authentication: Authorization and authentication are dynamically enforced for all resources through rigorous and adaptive mechanisms. Organizations adopting ZTA often employ ICAM systems and MFA for enhanced security.
- Information logging: To strengthen its security posture, the organization gathers comprehensive data regarding network and communication states.

Aims of the ZTA in Supply Chain

ZTA in the supply chain seeks to improve security by removing implicit trust and continuously verifying every user and device. It enforces strict access controls, minimizes risk through least-privilege principles, and protects against data breaches and cyberattacks. ZTA ensures secure, real-time collaboration across complex supply chain networks. The aims of the ZTA are as follows:

- Develop zero-trust algorithms: Using TensorFlow, create sophisticated ML-based zero-trust algorithms for real-time threat detection, dynamic access control, and continuous authentication that are specific to the financial cybersecurity of SMEs.
- Implement SMPC protocols: Guarantee the privacy of data and the security of transactions by integrating secure multiparty computing protocols to conduct sensitive financial calculations securely between organizations.
- Testing and validation: To guarantee scalable and practical solutions, verify and test the algorithms thoroughly in both virtual and physical SME settings, including detection accuracy, FPR, and computing efficiency.

Logical Components on Zero Trust

Implementing Zero Trust Architecture (ZTA) in an organization involves several interconnected processes. You may use these parts. Several interconnected processes are involved in implementing ZTA in a company.[22] These elements may be integrated into on-premises or cloud-based systems. Two logical components, the policy administrator and the PDP, are shown in Figure 5. Application data transmission occurs on this plane, as opposed to the ZTA logical components' separate control plane.

Here are the logical components of zero trust descriptions:

- This section is in charge of determining if a certain topic may use a specific resource. The PE utilizes an algorithm that considers both internal company regulations and external data to establish who has access to the resource.
- This component is in charge of starting and stopping lines of communication between a topic and a resource. This is a good method for creating session-specific authentications, tokens, and predestinations that customers use to access company resources.
- Connections between subject-to-enterprise resources must be initiated, monitored, and terminated as part of their lifetime management. For the PEP to get policy changes and/or relay requests, it connects to the PA.

BC-BASED SCM

Several of the present operational issues may be solved using BC technology, which offers a number of benefits when applied to traditional supply chain procedures. To begin with, the traditional. Since all supply chain participants use the same database, no one can see what the others are doing.[23,24] The absence of information about the supply chain's operations not only makes matters worse

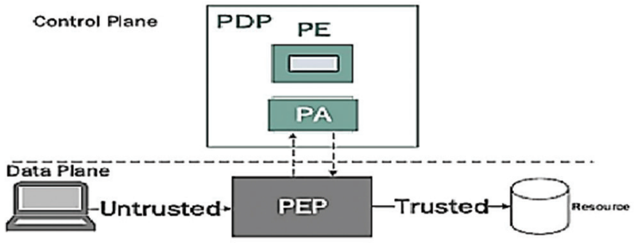

Figure 5: Core logical components of zero trust

in terms of trust and security, but it also causes greater instability in the transfer of goods and data between the different stakeholders. The present method also fails to adequately demonstrate compliance with norms and regulations due to the readily modifiable nature of data.[25] Serious risks to human and environmental health and safety could arise from the final product.

BC's Security in Supply Chain Context

The section explores the benefits and drawbacks of supply chain BC technology operations, providing a comprehensive overview:

- Ensuring tamper-proof data is crucial in supply chain operations, where each blockchain record must include an immutable timestamp to maintain integrity across multiple stakeholder interactions. The data are protected from any additional changes due to the timestamp, which guarantees its integrity.[26,27] A server that is reliable frequently employs applying the Time Stamp method to the blocks using the user's private key.
- One point of failure, one of the main benefits of Bitcoin BC, is decentralization. Information is retained by each node in the network. A singular point of failure can be mitigated by guaranteeing that a complete copy of the BC is on every node.
- The use of public-private keys, also known as asymmetric encryption, ensures that data remains secret while using BC technology. Each stakeholder is assigned a unique digital identity using the keys, which allows them to govern access to real-time data.
- Identity management: Supply chain stakeholders' digital identities are defined to guarantee data confidentiality. This information should only be accessible to permitted personnel. Multiple approaches exist for the management of digital identities. As an example, the model was suggested by a research study that used a secure cryptography-based clustering mechanism. This mechanism generates signatures and verifies them. To begin, all stakeholders' digital identities may be handled by a single body.
- SCM is the integration of BC technology with smart contracts, which is essential for optimizing the supply chain operation. A specific, predefined scenario triggers the execution of this code. This article proposes a smart contract trigger that initiates the money payment process and leads to the subsequent step.

BC Technology based on Supply Chain Security

Supply chains have become increasingly globalized, offering advantages such as reduced costs, greater efficiency, and access to broader markets. Yet, major problems with openness and security have also emerged as a result. Traditional supply chain systems are often plagued by inefficiencies, a lack of visibility, and vulnerability to fraud and errors. A study by IBM found that 71% of businesses consider supply chain visibility and transparency a significant challenge. These problems may cause financial losses, reputational damage, and legal repercussions, especially in sectors where regulatory compliance and product authenticity are crucial. BC aims to fix these issues by helping to track the supply chain, increase security, and promote openness, due to its decentralized and unaltered ledger. Despite more people being interested in BC applications in SCM, comprehensive research on the subject is lacking.[28-30] Researchers have mainly investigated how BC could be beneficial in theory, but there is not much information available about its performance in real situations. Research shows the benefits of BC for improving traceability and cutting down on fraud, but there is not much research about how it could be implemented, integrated with current technologies, and its lasting role. Furthermore, the impact of BC on different aspects of supply chain performance, such as cost reduction, efficiency gains, and stakeholder trust, remains underexplored.

CASE STUDIES IN CYBERSECURITY FOR SCM

This section provides examples from the real world that show how IAM, ZTA, and BC technologies have been successfully applied to supply chain maintenance.[31] These examples highlight practical applications, benefits, and outcomes of integrating advanced cybersecurity measures into SCM.

Strengthening Retail SCM with IAM: The IBM and Retail Corporation Example

A retail business with an international presence collaborated with IBM to add advanced IAM to defend its supply chain. Because there are many suppliers, warehouses, and logistics partners working daily, providing secure access to digital platforms was a growing challenge.[32] Thanks to multifactor authentication, access rights controlled by role and single sign-on, all systems could be managed to provide access for users within a single center. It created much less opportunities for the wrong people to access the system. By including IAM with supplier portals, only users confirmed by the system could see the inventory and time schedules for shipping or delivery, thus raising cybersecurity and making operations more efficient.

Implementing Zero Trust at Scale: Coca-Cola's Security Transformation

Coca-Cola used ZTA to secure its worldwide and sprawling supply chain.[33] Since cyber threats are now focused on Coca-Cola's trusted internal networks, the company now approaches everything as "never trust, always verify." By dividing its networks, checking all user identities meticulously, and continuously watching its traffic, Coca-Cola limited movement across its systems and boosted the protection of data in procurement, logistics, and distribution. Having endpoint verification and micro-segmentation in both their cloud and on-premise networks stopped unauthorized access to sensitive supply chain applications.

Enhancing Food Traceability with BC: Walmart and IBM Food Trust

IBM and Walmart unveiled IBM Food Trust, a BC-based initiative to make food safer and easier to trace. Walmart began using the technology to keep tabs on how food gets from the farms to its stores, hour by hour. For example, the length of time required to identify the location of imported mangoes fell dramatically from 7 days to only 2.2 s. It became easier for the company to respond to foodborne illness cases and follow important health requirements. Since all transactions on BC are unchangeable, the risk of data manipulation has decreased, and both consumers and regulators have begun to trust the technology more.

BC for Logistics Integrity: FedEx and the Shipment Verification Challenge

FedEx has used BC to boost transparency in the shipping industry and prevent fraud. Since every part of shipment handling is recorded on a BC ledger, such as checking at customs, warehouse transfers, and scanning, FedEx can prove how its shipments are handled. As a result, few disputes arise over damaged or lost goods because you can trace each package through the audit trail. As a result of BC's decentralized approach, everyone in the supply chain, encompassing outside carriers and regulators, can view and rely on secure shipping data, which helps resolve issues more quickly and increases reliability.

LITERATURE REVIEW

This section offers relevant cybersecurity work in SCM: The role of IAM, Zero Trust, and BC. The summaries of the literature reviews mentioned below are also shown in Table 1:

Sowan *et al*. (2025) present that Supply Chain Industry 4.0 is a global transformation that integrates digital technologies and interconnected networks, thereby improving operational efficiency and global reach. However, it also presents cyber risks such as ransomware, phishing attacks, and supply chain poisoning. Technologies such as BC, federated learning, trusted execution environments, and AI improve resilience. This paper analyzes the complexities of Supply Chain Industry 4.0, highlighting its effectiveness in security protocols, interoperability gaps, and the mitigation vulnerabilities.[34]

Beevi *et al*. (2025) proposed a framework for improving supply chain security and delivery efficiency by combining ant colony optimization and BC technology. The approach aims to eliminate inconvenient path design in last-mile delivery, ensuring a single delivery person handles multiple purchasers in the same area. The framework uses BC technology for security, transparency, and traceability, and advanced cybersecurity measures such as root of trust and PUFs. This scalable and reliable framework ensures operational efficiency

Table 1: Summary of cybersecurity in supply chain management

Author	Study focus	Key contributions	Challenges	Limitations	Future gap
Sowan *et al*. (2025)	Cybersecurity in Supply Chain Industry 4.0	Highlights cyber risks (e.g., ransomware, phishing), promotes technologies such as blockchain, AI, and federated learning	Interoperability gaps, cyber-attack resilience	General analysis: lacks implementation framework	More empirical studies are needed on tech integration impact
Beevi *et al*. (2025)	Blockchain and ACO for last-mile delivery	Proposes a secure, efficient framework using ACO + blockchain for smart logistics	Path optimization in dynamic environments	Focused on last-mile only; real-time scalability not tested	Expand the framework to the full supply chain lifecycle
Ettaloui *et al*. (2024)	Blockchain in the pharmaceutical supply chain	Builds a decentralized model to ensure traceability and security in pharma SCM	Data integrity and trust management	Domain-specific (pharmaceutical); limited scalability evidence	Generalize the approach to other critical supply chains
Balekundri *et al*. (2023)	Ethereum blockchain in the food supply chain	FARMSUPPLY model using smart contracts for traceability and trust	Managing heterogeneous data across the chain	Ethereum's transaction cost and speed	Explore hybrid blockchain or Layer-2 solutions
Muller (2022)	Cyber Supply Chain Risk Management (C-SCRM)	Stresses on cross-organizational cooperation and governance for cyber resilience	Third-party vulnerabilities, lack of standardization	Theoretical; lacks real-world implementation validation	Need pilot programs with collaborative governance structures
Ofori-Yeboah *et al*. (2021)	Financial analysis of cybersecurity investment in SCM	Combines NPV, IRR, Payback with cybersecurity ROI; includes IAM and behavioral analytics	Balancing cost vs. security impact	Financial focus may overlook technical feasibility	Explore the long-term security performance of proposed investment models

SCM: Supply chain management, ROI: Return on investment, IAM: Identity and access management, AI: Artificial intelligence, ACO: Ant colony optimization

and security in smart logistics and e-commerce applications.[35]

Ettaloui *et al*. (2024) propose a solution by introducing a BC-based model for pharmaceutical SCM. Capitalizing on the decentralized and transparent features inherent in BC technology, our model aims to effectively address the aforementioned challenges and elevate the overall efficiency and integrity of the pharmaceutical supply chain. This research significantly contributes to the integration of innovative technologies, such as BC, to mitigate risks and establish a safer and more reliable pharmaceutical supply chain.[36]

Balekundri *et al*. (2023) proposed that distributed ledger technology is transforming SCM by enhancing traceability, coordination, and funding access. In the food supply chain (FSC), BC is being used to improve results. A model called FARMSUPPLY uses Ethereum BC and smart contracts to verify and validate attributes at each stage of the FSC, providing a better view of farmers, products, and retailers.[37]

Muller (2022) provides a nuanced understanding of C-SCRM strategies that extend beyond the internal operations and technology of individual firms. The analysis highlights how crucial cross-organizational alignment and cooperation are to enhancing throughout the supply chain, cyber resilience. Key threat vectors, such as third-party vulnerabilities, a lack of standardized protocols, and information asymmetry, are outlined to raise awareness. The paper concludes with actionable recommendations for broader industry acceptance, highlighting the role of shared governance models and information-sharing mechanisms in mitigating systemic cyber risks.[38]

Ofori-Yeboah *et al*. (2021) assess the strategic and financial consequences of spending money on supply chain cybersecurity. Their contribution is threefold: First, they conduct a holistic review of the cyber threat landscape within SCM ecosystems, incorporating technologies such as IAM and behavioural analytics. Second, the paper employs the NPV, IRR, and Payback Period metrics to provide a multi-faceted evaluation of cybersecurity investments. Finally, the study proposes investment strategies that not only enhance security but also ensure business continuity and maximize long-term returns on investment. This integrated financial-security model supports decision-makers in balancing risk mitigation with operational performance.[39]

Table 1 summarises recent studies on cybersecurity in SCM, highlighting important areas of focus, contributions, challenges, limitations, and gaps in the field.

CONCLUSION AND FUTURE WORK

Supply chains that are becoming more digital and connected have brought major cybersecurity issues that must be addressed with complete and adjustable security solutions. The current paper outlines the main points of cybersecurity in the supply chain and how IAM helps manage access and limit hazards. Using ZTA has been found to greatly increase security by repeating trust checks during every user session. Even though BC technology offers improvements in visibility, traceability, and stakeholder trust, additional studies are required to fully achieve its aims in terms of cost reductions and increased efficiency. The case studies discussed show how different problems are handled and how solutions are applied. In the future, attention should be given to designing security frameworks that bring together IAM, ZTA, BC, and artificial intelligence and machine learning to help detect and deal with upcoming threats before they become significant. It is also necessary to find scalable and interoperable options that can handle the challenges of global supply chains to help strengthen the supply chain and preserve trust when more supply chain work moves online.

REFERENCES

1. Boyson S. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation 2014;S34:342-53
2. Wang Y, Han JH, Beynon-Davies P. Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. Supply Chain Manag An Int J 2018;24:62-84.
3. Murugandi K. End-to-end SAP implementation in global supply chains : Bridging functional and technical aspects of EDI integration. Int J Res Anal Rev 2021;8:894-900.
4. Queiroz MMintegration: A, Telles R, Bonilla SH. Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Manag 2020;25:241-54.
5. Mendling J, Weber I, Van Der Aalst W, Vom Brocke J, Cabanillas C, Daniel F. Blockchains for business process management - challenges and opportunities. ACM Trans Manag Inf Syst 2018;9:1-16.
6. Prajapati V. Exploring the role of digital twin technologies in transforming modern supply chain management. Int J Sci Res Arch 2025;14:1387-95.
7. Ghadge A, Weiß M, Caldwell N, Wilding R. Managing cyber risk in supply chains: A review and research agenda. Supply Chain Manag An Int J 2019;25:223-40.
8. Prajapati V. Enhancing supply chain resilience through machine learning- based predictive analytics for demand forecasting. Int J Sci Res Comput Sci Eng Inf Technol 2025;11:345-54.
9. Thomas Jubin SG, Vedi KV. Enhancing supply chain resilience through cloud-based SCM and advanced machine learning : A case study of logistics. J Emering Technol Innov Res 2021;8:357-64.
10. Chatterjee S. Mitigating supply chain malware risks in operational technology : Challenges and solutions for the oil and gas industry. J Adv Dev Res 2021;12:1-12.
11. Polinati AK. AI-powered anomaly detection in cybersecurity: Leveraging deep learning for intrusion prevention. Int J Commun Netw Inf Secur 2025;17:13.
12. Balasubramanian A. Improving legacy software quality through AI-driven code smell detection. ESP J Eng Technol Adv 2021;1:245-53.
13. Prajapati N. Federated learning for privacy-preserving cybersecurity : A review on secure threat detection. Int J Adv Res Sci Commun Technol 2025;5:520-8.
14. Thomas J, Patidar P, Vedi KV, Gupta S. An analysis of predictive maintenance strategies in supply chain management. Int J Sci Res Arch 2022;6:308-17.
15. Garg S. Predictive analytics and auto remediation using artificial inteligence and machine learning in cloud computing operations. Int J Innov Res Eng Multidiscip Phys Sci 2019;7:1-5.
16. Thangaraju V. Security considerations in multi-cloud environments with seamless integration: A review of best practices and emerging threats. Trans Eng Comput Sci 2024;12:226-38.
17. Gogineni A. Observability driven incident management for cloud-native application reliability. Int J Innov Res Eng Multidiscip Phys Sci 2021;9:1-10.
18. Neeli SS. Transforming data management: The quantum computing paradigm shift. Int J Lead Res Publ 2021;2:7.
19. Gogineni A. Multi-cloud deployment with kubernetes: Challenges, strategies, and performance optimization. Int Sci J Eng Manag 2022;1:1-6.
20. Seetharaman KM. End-to-End SAP implementation in global supply chains : Bridging functional and technical aspects of EDI integration. Int J Res Anal Rev 2021;8:2201-6.
21. Karabacak B, Whittaker T. Zero Trust and Advanced Persistent Threats: Who will Win the War? In: Proceedings of the 17th International Conference on Cyber Warfare and Security; 2022.
22. Abhishek A, Khare P. Cloud security challenges: Implementing best practices for secure SaaS application development. Int J Curr Eng Technol 2021;11:669-76.
23. Murugandi K, Seetharaman R. Analysing the role of inventory and warehouse management in supply chain agility : Insights from retail and manufacturing industries. Int J Curr Eng Technol 2022;12:583-90.
24. Goyal A. Integrating blockchain for vendor coordination and agile scrum in efficient project execution. Int J Innov Sci Res Technol 2024;9:1768-78.
25. Al-Farsi S, Rathore MM, Bakiras S. Security of blockchain-based supply chain management systems: Challenges and opportunities. Appl Sci 2021;11:5585.

26. Pandya S. Advanced blockchain-based framework for enhancing security, transparency, and integrity in decentralised voting system. Int J Adv Res Sci Commun Technol 2022;2:865-76.
27. Pandya S. Innovative blockchain solutions for enhanced security and verifiability of academic credentials. Int J Sci Res Arch 2022;6:347-57.
28. Pandya S. A systematic review of blockchain technology use in protecting and maintaining electronic health records. Int J Res Anal Rev 2021;8:421-6.
29. Modalavalasa G. Advanced blockchain mechanisms for strengthening data security and ensuring privacy in decentralized systems. Int J Recent Technol Sci Manag 2023;8:89-98.
30. Chatterjee P. Smart contracts and machine learning: Exploring blockchain and AI in fintech. Indian J Sci Technol 2025;18:113-24.
31. Dhamdhere M, Karande S. Identity and access management: Concept, challenges, solutions. Int J Latest Trends Eng Technol 2016;8:300-8.
32. Latif MN, Aziz NA, Hussin NS, Aziz ZA. Cyber security in supply chain management: A systematic review. Logforum 2021;17:49-57.
33. Hassija V, Chamola V, Gupta V, Jain S, Guizani N. A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet Things J 2020;8:6222-46.
34. Sowan BI, Zighan S, Altarawneh A. Supply Chain 4.0: Driving Operational Efficiency, Resilience, and Cybersecurity Using Advanced Technologies. In: 2025 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA); 2025. p. 1-8.
35. Beevi LS, Bhama PK, Vijayan JA, Dani JP, Premalatha J. Optimizing Supply Chain Security Using ACO and Blockchain: Integrating Root of Trust, Unclonable Functions, and SBOM for Cybersecurity. In: 2025 International Conference on Visual Analytics and Data Visualization (ICVADV); 2025. p. 264-9.
36. Ettaloui N, Arezki S, Gadi T. Enhancing Pharmaceutical Supply Chain Management: A Blockchain-Based Model. In: 2024 IEEE 15th International Colloquium on Logistics and Supply Chain Management (LOGISTIQUA); 2024. p. 1-6.
37. Balekundri O, Tigadi R, Jayakkanavar A. FARMSUPPLY: Food Supply Chain Management using Blockchain Technology. In: 3rd IEEE International Conference on Technology, Engineering, Management for Societal Impact using Marketing, Entrepreneurship and Talent, TEMSMET 2023; 2023.
38. Muller SR. Analyzing Deficits in Awareness Among Chief Supply Chain Officers Who Have Not Adopted Cybersecurity as a Threat to Supply Chains. In: 2022 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT), IEEE; 2022. p. 1-6.
39. Ofori-Yeboah A, Addo-Quaye R, Oseni W, Amorin P, Agangmikre C. Cyber Supply Chain Security: A Cost Benefit Analysis Using Net Present Value. In: 2021 International Conference on Cyber Security and Internet of Things (ICSIoT), IEEE; 2021. p. 49-54.