Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

INTEGRATING BLOCKCHAIN, AI, AND RFID TECHNOLOGIES TO COMBAT COUNTERFEITING IN SUPPLY CHAIN MANAGEMENT: A COMPREHENSIVE LITERATURE REVIEW

Muhammad Khairul Zharif Nor A'zam[1*], Mohd Hilal Muhammad[2], Ahmad Afif Ahmarofi[3], Mohd Zhafri Mohd Zukhi[4], Suheil Che Sobry[5], Ahmad Harith Ashrofie Hanafi[6]

[1] College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA (UiTM) Kedah Branch, Malaysia
Email: khairulzharif@uitm.edu.my
[2] College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA (UiTM) Kedah Branch, Malaysia
Email: hilalmuhd@uitm.edu.my
[3] College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA (UiTM) Kedah Branch, Malaysia
Email: ahmadafif@uitm.edu.my
[4] College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA (UiTM) Kedah Branch, Malaysia
Email: zhafri319@uitm.edu.my
[5] Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Kedah Branch, Malaysia
Email: suheil@uitm.edu.my
[6] Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Kedah Branch, Malaysia
Email: ashrofie@uitm.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 05.01.2025
Revised date: 18.01.2025
Accepted date: 25.02.2025
Published date: 13.03.2025

To cite this document:

Nor A'zam, M. K. Z., Muhammad, M. H., Ahmadrofi, A. A., Zukhi, M. Z. M., Che Sobry, S., & Hanafi, A. H. A. (2025). Integrating Blockchain, AI,

Abstract:

Counterfeiting in supply chain management poses significant challenges, including economic losses, compromised product safety, and damage to brand reputation. The increasing complexity and globalization of supply chains have exacerbated these issues, making it difficult for organizations to ensure the authenticity and traceability of products. The purpose of this research is to investigate how blockchain, AI, and RFID technologies can be used to provide complete protection against supply chain counterfeiting. Blockchain guarantees tamper-proof transaction records by ensuring decentralization, immutability, and transparency. Real-time tracking and physical-layer identification made possible by RFID help to lower the risk of fake products finding their way onto the supply chain. Through pattern analysis, automated verification, and anomaly identification suggesting fraudulent activity,

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

And RFID Technologies To Combat Counterfeiting In Supply Chain Management: A Comprehensive Literature Review. *Journal of Information System and Technology Management, 10* (38), 87-118.

DOI: 10.35631/JISTM.1038007

artificial intelligence improves detection capacity. The findings reveal that the integration of these technologies creates a robust framework for ensuring end-to-end traceability, enhancing security, and improving operational efficiency. For instance, IoT-based secure medicine supply chains and electronic component authentication systems demonstrate the practical effectiveness of this approach. Despite its promise, challenges such as technical complexity, scalability, and adoption barriers remain. These include the need for secure communication protocols between RFID tags and blockchain nodes, as well as the cost and expertise required for implementation. This study has important ramifications since the suggested structure not only solves the immediate problem of counterfeiting but also creates the basis for more open, effective, and strong supply networks. Future research should focus on overcoming these challenges by developing scalable solutions, cost-effective implementations, and standardized regulatory frameworks. Organizations that use Blockchain, AI, and RFID can dramatically reduce the risk of counterfeit items, ensuring the legitimacy and safety of commodities from manufacture to distribution.

Keywords:

Artificial Intelligence (AI); Blockchain; RFID; Supply Chain;

Introduction

In an era of globalization, supply chain management has grown increasingly complex as goods traverse multiple jurisdictions and stakeholders before reaching end consumers. While this complexity fosters economic growth, it also creates vulnerabilities, particularly in the form of counterfeit products infiltrating supply chains. Counterfeiting not only erodes consumer confidence but also poses significant dangers to public health, safety, and intellectual property rights (Islam, Shen, & Badsha, 2022; Pandey & Singh, 2024). The spread of counterfeit goods has been worsened by an absence of transparency and traceability in traditional supply chain systems, necessitating novel technical solutions.

Recent developments in digital technologies have cleared the way for transformational approaches to supply chain management. Blockchain, artificial intelligence (AI), and radio-frequency identification (RFID) have emerged as promising tools to address the challenges posed by counterfeiting. Blockchain provides decentralization, immutability, and transparency, allowing for safe and secure record-keeping (Kamble & Joshi, 2024; Onu, Mbohwa, & Pradhan, 2024). RFID facilitates real-time tracking and physical-layer authentication, while AI enhances detection capabilities and automates verification processes (Banu et al., 2024; Wang et al., 2023). Together, these technologies hold the potential to revolutionize supply chain integrity and effectively combat counterfeiting.

Despite their individual strengths, the fragmented adoption of these technologies has limited their effectiveness in addressing the multifaceted issue of counterfeiting. Traditional supply chains often suffer from isolated data systems, a lack of interoperability, and inadequate security measures, making them vulnerable to counterfeit infiltration (Lobachev, Mahmoud, & Patooghy, 2022). Furthermore, the absence of a unified framework that integrates blockchain, AI, and RFID into a cohesive solution has hindered progress in this domain. As a result, counterfeit items continue to have a significant influence on businesses, including pharmaceuticals, electronics, and luxury goods, resulting in billions of dollars in losses each year (Chinchmalatpure et al., 2024).

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Numerous studies have explored the application of blockchain, AI, and RFID technologies in isolation to combat counterfeiting. For instance, blockchain-based systems have been shown to improve traceability and transparency in supply chains (Pandey & Singh, 2024; Kamble & Joshi, 2024). Similarly, RFID technology has demonstrated its capability to offer real-time tracking and cost-efficient implementation (Wang et al., 2023). Meanwhile, AI-driven models have proven effective in detecting anomalies and automating verification processes (Banu et al., 2024). Few studies have investigated the combined possibility of integrating these technologies into a seamless framework.

While the individual contributions of blockchain, AI, and RFID have been extensively documented, there is still a crucial gap in understanding how these technologies may be effectively linked to create a significant anti-counterfeiting system. Existing literature often focuses on isolated applications without addressing the technical and operational challenges associated with their combined implementation (Sidorov et al., 2019). Moreover, there is limited exploration of case studies and real-world implementations that demonstrate the practical feasibility of such integrated solutions (Lobachev et al., 2022).

This paper aims to address the aforementioned research gap by conducting a comprehensive literature review on the integration of blockchain, AI, and RFID technologies to combat counterfeiting in supply chain management. Specifically, it seeks to: (1) review the benefits and challenges of blockchain, AI, and RFID technologies; (2) explore the synergistic potential of integrating these technologies; and (3) examine the connection between supply chain security concepts and key themes such as AI integration, blockchain technology, and RFID technology.

This study makes several key contributions to the field. First, it provides a holistic overview of how blockchain, AI, and RFID can complement one another to create a multi-layered defense against counterfeiting. Second, it synthesizes findings from recent studies to highlight successful implementations and identify unresolved challenges. Finally, it offers actionable insights for practitioners and policymakers seeking to adopt these technologies in their supply chain operations.

The remaining section of this paper is organized as follows. The literature review section provides a thorough summary of current research on anti-counterfeiting technologies in supply chain management, particular emphasis on blockchain, AI, and RFID. The methodology part examines the fundamental ideas of these technologies, focusing on their functions in supply chain management. The results and discussion part investigates the integration of different technologies, emphasizing their combined benefits and problems. Finally, the conclusion section summarizes the important findings and their implications for practice.

Literature Review

The growing prevalence of counterfeit goods in global supply chains has prompted extensive research into technological solutions aimed at enhancing transparency, traceability, and security. Past studies have explored various technologies, including block-chain, AI, and RFID, to address the challenges posed by counterfeiting. A summary of key findings from these studies is presented in Table 1, which highlights their contributions, methodologies, and implications for supply chain management. These findings underscore the transformative

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

potential of integrating these technologies into a cohesive framework to combat counterfeiting effectively.

Table 1: The Summary Of Key Findings Of Past Studies

Authors	Technology	Key Contribution	Implications
Kamble & Joshi (2024)	Blockchain	Enhanced traceability through decentralized, tamper-proof ledgers	Improved transparency and trust among supply chain stakeholders
Pandey & Singh (2024)	Blockchain	Ensured data integrity and accountability	Strengthened regulatory compliance and consumer confidence
Wang et al. (2023)	RFID	Enabled real-time tracking and automated inventory management	Reduced operational inefficiencies and minimized human error
Banu et al. (2024)	RFID + AI	Enhanced anomaly detection using AI-driven models	Proactive identification of counterfeit products
Lobachev et al. (2022)	AI	Automated verification and predictive analytics	Enabled dynamic responses to emerging supply chain threats
Sidorov et al. (2019)	Integration	Identified interoperability challenges in combining blockchain, AI, and RFID	Highlighted the need for unified frameworks

Blockchain technology has been widely studied for its ability to provide decentralized, immutable, and transparent record-keeping systems. Kamble and Joshi (2024) demonstrated that blockchain enhances traceability by creating tamper-proof ledgers that document every transaction within a supply chain. Similarly, Pandey and Singh (2024) highlighted blockchain's role in fostering trust among stakeholders by ensuring data integrity and accountability. These

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
findings are consistent with the theoretical framework of the Information Systems Success Model (DeLone & McLean, 1992), which emphasises the significance of system quality, information quality, and user happiness in obtaining desired results. In the context of anti-counterfeiting, blockchain's ability to ensure high-quality, reliable data directly contributes to improved supply chain performance.

RFID technology has also been extensively researched for its capacity to enable real-time tracking and authentication of physical goods. Wang et al. (2023) found that RFID systems significantly reduce operational inefficiencies by automating inventory management and minimizing human error. Furthermore, Banu et al. (2024) demonstrated that RFID integration with AI-driven models enhances anomaly detection, enabling proactive identification of counterfeit products. These findings align with the Technology Acceptance Model (TAM) (Davis, 1989), which suggests that perceived usefulness and simplicity of use impact the adoption of new technologies. The practical feasibility and cost-effectiveness of RFID systems make them highly acceptable in industries such as retail and pharmaceuticals.

Artificial intelligence complements both blockchain and RFID by providing advanced analytical capabilities. Lobachev, Mahmoud, and Patooghy (2022) explored AI's role in automating verification processes and detecting patterns indicative of counterfeit infiltration. Their study revealed that machine learning algorithms could predict vulnerabilities in supply chains, thereby enabling preemptive measures. This is consistent with the Dynamic Capabilities Theory (Teece, Pisano, & Shuen, 1997), which highlights the need for organizations to adapt and innovate in response to environmental changes. AI's predictive and adaptive capabilities empower supply chains to respond dynamically to emerging threats.

Despite the individual strengths of these technologies, their fragmented adoption has limited their effectiveness. Sidorov et al. (2019) identified interoperability challenges as a significant barrier to integrating blockchain, AI, and RFID into a unified framework. Building on this, the current study uses the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003) as its theoretical underpinning. UTAUT offers a complete lens for assessing how performance expectancy, effort expectancy, social impact, and facilitating factors affect the adoption of integrated anti-counterfeiting systems. By managing these issues, the study seeks to close the gap between discrete applications and a comprehensive technological solution.
In summary, past research has laid a strong foundation for understanding the individual contributions of blockchain, AI, and RFID in combating counterfeiting. However, the lack of integration frameworks remains a critical limitation. The present study builds on these insights by proposing a unified approach that leverages the synergistic potential of these technologies. By grounding the research in established theoretical frameworks, this study aims to provide actionable recommendations for practitioners and policymakers seeking to enhance supply chain security.

Methodology

This study employed a systematic and data-driven approach to address the stated objectives, leveraging insights from recent academic publications indexed in Scopus utilizing Scopus AI. The methodology is structured to ensure a comprehensive analysis of the benefits and challenges of blockchain, AI, and RFID technologies (Objective 1), an exploration of their synergistic potential when integrated (Objective 2), and an examination of the connection

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
between supply chain security and key themes such as AI integration, blockchain technology, and RFID technology (Objective 3).

To achieve these objectives, the study utilized Scopus AI, combining natural language queries and keyword-based search strategies. The natural language query, “How to integrate Blockchain, AI, and RFID Technologies to Combat Counterfeiting in Supply Chain Management?” was employed to capture a broad spectrum of literature. This was supplemented with a keyword search using the following terms: ("blockchain" OR "distributed ledger" OR "crypto*") AND ("artificial intelligence" OR "AI" OR "machine learning") AND ("RFID" OR "radio frequency identification" OR "tagging") AND ("supply chain" OR "logistics" OR "inventory") AND ("counterfeiting" OR "fraud" OR "forgery" OR "piracy"). This dual approach ensured comprehensive coverage of literature addressing the research objectives.

For Objective 1, the study began by identifying foundational concepts and applications of each technology within the context of supply chain management. Blockchain technology was analyzed for its decentralization, immutability, and transparency, which collectively enhance traceability and reduce the risk of counterfeit products entering the supply chain (Pandey & Singh, 2024; Kamble & Joshi, 2024). Similarly, RFID technology was examined for its real-time tracking capabilities, cost-effective implementation, and physical-layer authentication, which contribute to enhanced supply chain visibility (Wang et al., 2023; Islam et al., 2022). AI's role was explored through its ability to detect anomalies, automate verification processes, and integrate seamlessly with blockchain for multi-layered defense against counterfeiting (Banu et al., 2024). Challenges such as technical complexity, adoption barriers, and the need for significant computational power were also critically assessed to provide a balanced perspective on the feasibility of implementing these technologies.

For Objective 2, the study delved into the synergistic potential of integrating blockchain, AI, and RFID technologies. By synthesizing findings from case studies and real-world implementations, the research highlighted how these technologies complement one another to create a robust anti-counterfeiting framework. For instance, RFID tags provide real-time data updates at various checkpoints, AI algorithms analyze this data to identify irregularities, and blockchain ensures the integrity and transparency of recorded transactions (Lobachev et al., 2022; Onu et al., 2024). This tripartite integration not only enhances supply chain security but also streamlines administrative activities, making it a transformative solution for modern supply chains.

Finally, to address Objective 3, the study examined the broader implications of supply chain security by connecting it to the key themes of AI integration, blockchain technology, and RFID technology. Supply chain security was conceptualized as a multifaceted issue that requires both digital and physical safeguards. Blockchain’s decentralized ledger system ensures tamper-proof record-keeping, while AI-driven models enhance detection capabilities and predictive analytics. Meanwhile, RFID technology bridges the gap between digital records and physical goods, ensuring end-to-end traceability. Together, these technologies address critical vulnerabilities in supply chain security, such as counterfeit infiltration, intellectual property theft, and lack of transparency (Chinchmalatpure et al., 2024; Sidorov et al., 2019). By mapping these connections, the study underscores the importance of adopting an integrated technological approach to safeguard supply chains effectively.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

The methodological rigor of this study is further strengthened by its reliance on high-quality, peer-reviewed sources from Scopus AI, ensuring the credibility and relevance of the findings. Through this structured approach, the study provides actionable insights into the individual and collective contributions of blockchain, AI, and RFID technologies, paving the way for future research and practical applications in supply chain management.

Result and Discussion

This section presents the findings of the study in alignment with the research objectives, offering a comprehensive analysis of how Blockchain, AI, and RFID technologies can combat counterfeiting in supply chain management. By employing a systematic and technology-driven approach, the results integrate insights from these three technologies, highlighting their roles, interdependencies, and collective impact. The discussion contextualizes these findings within the broader academic literature, emphasizing key themes such as decentralization, real-time tracking, automated verification, and multi-layered security. It also explores emerging trends in technology integration, persistent challenges like scalability and adoption barriers, and actionable strategies to address these issues. Through this analysis, the study underscores the transformative potential of integrating Blockchain, AI, and RFID to enhance supply chain security, transparency, and efficiency while reducing counterfeiting risks and ensuring product authenticity.

To Review the Benefits and Challenges of Blockchain, AI, and RFID Technologies

The analysis of Blockchain, AI, and RFID technologies indicates their disruptive potential for combating counterfeit in supply chain management. Blockchain is notable for its decentralization, immutability, and transparency, which significantly improve traceability and lessen the possibility of counterfeit products penetrating the supply chain. These features ensure that all transactions are securely recorded and available to all stakeholders, promoting confidence and accountability (Pandey & Singh, 2024; Kamble & Joshi, 2024). Furthermore, smart contracts—an important component of blockchain—automate and enforce quality standards, reducing the chance of counterfeit items entering the supply chain (Banu et al., 2024). However, implementing blockchain is not without its obstacles. Technical complexity, scaling concerns, and the requirement for large computational capacity are all obstacles to deployment (Lobachev et al., 2022). Resistance from organizations due to costs and the need for process overhauls further highlights the importance of addressing these barriers to facilitate widespread adoption.

RFID technology complements blockchain by providing real-time tracking and physical-layer authentication, making it a critical component in anti-counterfeiting efforts. RFID tags can be scanned at various checkpoints in the supply chain, updating the product’s status on the blockchain and enabling real-time visibility (Wang et al., 2023). This capability not only enhances traceability but also ensures that physical tags are authenticated, making it harder for counterfeiters to clone or tamper with them (Islam et al., 2022). The cost-effectiveness of RFID tags further strengthens their appeal, as they can be easily integrated into existing supply chain systems (Chinchmalatpure et al., 2024). Despite these advantages, challenges such as the risk of tag cloning and integration complexity with blockchain systems must be addressed to maximize the technology's potential (Sidorov et al., 2019).

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Artificial intelligence (AI) plays a pivotal role in enhancing detection capabilities and automating verification processes within supply chains. AI-driven models, particularly those leveraging machine learning and deep learning, can analyze patterns and detect anomalies that may indicate the presence of counterfeit products (Banu et al., 2024). By automating verification processes, AI reduces the need for manual checks, thereby increasing efficiency and minimizing human error (Onu et al., 2024). Moreover, AI's integration with blockchain creates a multi-layered defense system, ensuring both digital and physical security (Kamble & Joshi, 2024). Nevertheless, the high computational power required for AI algorithms and the need for technical expertise present significant challenges. Organizations must invest in infrastructure and training to fully harness AI's capabilities, which could act as a barrier to adoption (Mandal et al., 2024).

When examining the collective benefits of these technologies, it becomes evident that their integration offers a comprehensive solution to counterfeiting. Blockchain ensures data integrity and transparency, RFID provides real-time tracking and physical authentication, and AI enhances detection and automation. Together, these technologies create a robust framework that addresses multiple vulnerabilities in supply chain security (Wang et al., 2023; Lobachev et al., 2022). For instance, RFID tags provide real-time updates, AI analyzes this data for irregularities, and blockchain ensures the immutability of recorded transactions. This synergy not only enhances supply chain security but also streamlines administrative activities, making it a transformative solution for modern supply chains (Onu et al., 2024).

Despite their individual and collective benefits, the adoption of these technologies faces several challenges that must be addressed to realize their full potential. Technical complexity, interoperability issues, and scalability concerns remain significant barriers, particularly when integrating blockchain, AI, and RFID into existing systems (Lobachev et al., 2022). Additionally, the cost of implementation and the need for organizational change management can deter companies from adopting these solutions (Chinchmalatpure et al., 2024). Future research should focus on developing scalable and cost-effective frameworks that address these challenges while ensuring regulatory compliance. By overcoming these hurdles, organizations can leverage the full potential of blockchain, AI, and RFID to combat counterfeiting and enhance supply chain security.

Having explored the individual benefits and challenges of Blockchain, AI, and RFID technologies in Objective (1), the focus now shifts to Objective (2), which examines their synergistic potential when integrated. The integration of these technologies highlights how they complement one another to create a more secure, transparent, and efficient supply chain ecosystem.

To Review Blockchain, AI, and RFID Technologies Synergistic Potential When Integrated

The integration of Blockchain, AI, and RFID technologies demonstrates significant synergistic potential in combating counterfeiting within supply chain management. Each technology brings unique strengths that, when combined, create a robust and multi-layered defense system. Blockchain ensures data integrity and transparency by providing a decentralized ledger where transactions are immutable and visible to all stakeholders (Pandey & Singh, 2024; Kamble & Joshi, 2024). This feature is complemented by RFID technology, which provides real-time tracking and physical-layer authentication, ensuring that the movement of goods is

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
continuously monitored and verified (Wang et al., 2023; Islam et al., 2022). AI enhances this framework by analyzing patterns, detecting anomalies, automating verification processes, and enabling predictive analytics to identify potential vulnerabilities (Banu et al., 2024). Together, these technologies form a comprehensive solution that addresses both digital and physical security challenges in supply chains.

One of the primary benefits of incorporating these technologies is their ability to reduce administrative processes while improving security. RFID tags, for example, can be read at multiple supply chain checkpoints to update the product's status on the blockchain in real time (Lobachev et al., 2022). AI algorithms then examine this data for anomalies, such as unauthorised alterations or inconsistencies, which could indicate counterfeit infiltration (Onu et al., 2024). The immutability of Blockchain ensures the integrity of recorded transactions, making counterfeiters' attempts to tamper with the data practically difficult. This seamless integration of RFID, AI, and Blockchain enhances traceability while simultaneously reducing the need for manual intervention, enhancing operational efficiency (Chinchmalatpure et al., 2024).

Real-world implementations further highlight the synergistic potential of these integrated technologies. For example, in medical supply chains, blockchain-enabled systems have been used to track the authenticity of pharmaceuticals, while RFID tags provide real-time updates on their location and condition (Chinchmalatpure et al., 2024). AI-driven models analyze this data to predict potential risks, such as temperature deviations or delays, ensuring that products remain safe and compliant throughout the supply chain (Wang et al., 2023). Similarly, in the electronics industry, AI-enabled authentication systems have been combined with blockchain and RFID to verify the legitimacy of components, reducing the risk of counterfeit parts entering the market (Banu et al., 2024). These case studies demonstrate the practical feasibility and effectiveness of integrating blockchain, AI, and RFID technologies.

Despite their synergistic potential, the integration of these technologies presents several challenges that must be addressed to maximize their impact. Technical complexity remains a significant barrier, particularly in ensuring interoperability between blockchain, AI, and RFID systems (Sidorov et al., 2019). Scalability issues and the need for substantial computational power further complicate implementation, especially for organizations with limited resources (Lobachev et al., 2022). Additionally, the cost of deploying RFID tags, developing AI algorithms, and maintaining blockchain networks can deter smaller enterprises from adopting these solutions (Mandal et al., 2024). Addressing these challenges requires innovative frameworks that balance cost-effectiveness with technical robustness, ensuring widespread adoption across industries.

In conclusion, the integration of blockchain, AI, and RFID technologies offers a transformative approach to combating counterfeiting in supply chain management. By combining blockchain’s transparency, RFID’s real-time tracking, and AI’s detection capabilities, organizations can create a secure and efficient system that addresses both digital and physical vulnerabilities (Onu et al., 2024). Real-world implementations have demonstrated the practical feasibility of these integrated solutions, highlighting their potential to revolutionize supply chain security. However, overcoming technical and financial barriers is crucial to realizing their full potential. Future research should focus on developing scalable and cost-effective

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
frameworks that facilitate the seamless integration of these technologies, paving the way for a more secure and transparent supply chain ecosystem.

Having explored the synergistic potential of Blockchain, AI, and RFID technologies in Objective (2), the focus now shifts to Objective (3), which examines how these innovations collectively strengthen supply chain security by addressing key themes such as AI-driven threat detection, blockchain-enabled transparency, and RFID-based real-time tracking.

To Examine the Connection between Supply Chain Security Concept with Key Themes such as AI Integration, Blockchain Technology, and RFID Technology

Figure 1 presents a concept map that highlights the key technologies and strategies contributing to supply chain security, focusing on three major domains: AI Integration, Blockchain Technology, and RFID Technology. Each of these domains plays a pivotal role in enhancing transparency, efficiency, and risk management within modern supply chains, addressing critical vulnerabilities such as counterfeiting, data tampering, and inefficiencies.

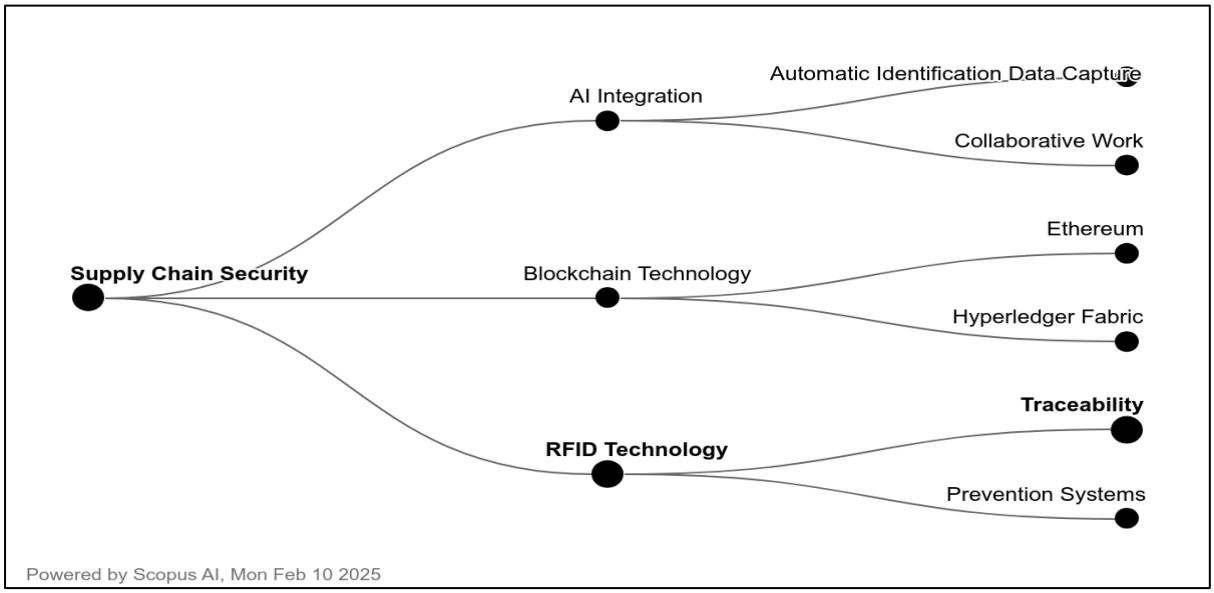

Figure 1: Scopus AI Concept Map for Key Technologies and Strategies that Contribute Towards Supply Chain Security

AI Integration is a cornerstone of supply chain security, particularly through its support of Automatic Identification and Data Capture (AIDC). Technologies such as barcode scanning, RFID, and computer vision enable real-time tracking and authentication of goods, ensuring accurate and up-to-date information across the supply chain. Additionally, AI-driven collaborative work fosters coordination among stakeholders, improving decision-making and enabling proactive risk mitigation. By automating processes and analyzing vast amounts of data, AI enhances operational efficiency and strengthens security measures.

Blockchain Technology provides decentralized and tamper-proof solutions for securing transactions and data exchanges within the supply chain. Platforms like Ethereum highlight the use of smart contracts, which automate secure and transparent transactions, reducing the need for intermediaries and minimizing the risk of fraud. Meanwhile, Hyperledger Fabric represents permissioned blockchain frameworks tailored for enterprise applications, ensuring controlled

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
access and maintaining data integrity. These blockchain solutions not only enhance trust among stakeholders but also create a robust foundation for traceability and accountability.

RFID Technology is essential for enabling real-time traceability, allowing organizations to monitor the movement of goods throughout the supply chain. This capability ensures accountability and improves inventory management, making it easier to identify discrepancies or irregularities. Additionally, RFID-based prevention systems play a critical role in safeguarding supply chains against counterfeiting, theft, and unauthorized access. By integrating RFID with other technologies, organizations can reinforce the reliability and security of their supply chain networks.

Overall, the concept map provides a structured overview of how emerging technologies are transforming supply chain security. The integration of AI, blockchain, and RFID creates a multi-layered defense system that addresses both digital and physical vulnerabilities. By leveraging these technologies, organizations can improve operational resilience, prevent fraud, and establish a more transparent and secure supply chain ecosystem.

Having established the connection between supply chain security and key themes such as blockchain and RFID technologies in Objective 3, the focus now shifts to exploring the specific linkage between supply chain security and AI integration for automatic identification and data capture. This section will highlight how AI-driven solutions enhance real-time monitoring, anomaly detection, and operational efficiency, further strengthening supply chain security.

Linkage between Supply Chain security to AI Integration for Automatic Identification Data Capture

Supply chain security is an important consideration in modern logistics, especially as supply networks grow more digitised and networked. One of the most effective approaches to improve supply chain security is to integrate Artificial Intelligence (AI) with Automatic Identification and Data Capture (AIDC) technology. AIDC systems, such as Radio Frequency Identification (RFID) and Unique Identification (UID), play an important role in increasing information flow across supply chains by allowing for real-time tracking and traceability of commodities (Hruska et al., 2019; Kelepouris et al., 2007). These technologies provide a foundation for secure and transparent operations, ensuring that data about the movement and status of products is accurate and reliable. However, integrating AI into these systems amplifies their capabilities, enabling advanced data analysis and decision-making processes that further enhance supply chain security.

The integration of AI into AIDC systems offers significant benefits, including enhanced visibility, traceability, and responsiveness across the supply chain. For instance, RFID tags can capture data at various checkpoints, which AI algorithms can then analyze to identify patterns, detect anomalies, and predict potential risks (Cook, 2005; Samayamantri, 2024). This combination allows organizations to respond proactively to disruptions or security threats, such as counterfeit infiltration or unauthorized access. Moreover, AI-driven analytics improve operational efficiency by automating routine tasks like inventory management and quality control, thereby reducing human error and increasing productivity. By leveraging AI's ability to process vast amounts of data quickly and accurately, supply chains can achieve higher levels of transparency and accountability—key components for maintaining robust security.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Despite these advantages, integrating AI with AIDC technologies presents several challenges that must be addressed to ensure robust supply chain security. Technological complexity and data privacy concerns are among the primary obstacles, as the digitization of supply chains increases the risk of cyberattacks and insider threats (Nguyen et al., 2024). For example, while AI enhances the ability to analyze and interpret data from AIDC systems, it also creates vulnerabilities if the data is not adequately protected. Additionally, implementing AI-powered solutions requires significant investment in infrastructure, technical expertise, and cybersecurity measures. Organizations must strike a balance between adopting advanced technologies and safeguarding sensitive information to mitigate these risks effectively.

The convergence of AI, AIDC, and blockchain technology offers a promising solution to many of these challenges. Blockchain provides a decentralized and immutable ledger that ensures the integrity and transparency of data captured by AIDC systems, while AI enhances the system's ability to analyze and act on this data in real time (Karai & Chroqui, 2024). For example, AIoT (Artificial Intelligence of Things) devices integrated with blockchain can optimize supply chain operations by enabling real-time monitoring, predictive maintenance, and automated verification processes. This tripartite integration not only strengthens supply chain security but also addresses issues related to scalability, interoperability, and regulatory compliance. By combining these technologies, organizations can create a multi-layered defense system that protects against both physical and digital threats.

Finally, the connections between supply chain security, AI integration, and automatic identification data capture demonstrate the revolutionary power of these technologies when combined. AIDC systems lay the groundwork for capturing and transferring data, while AI improves the ability to analyse and act on that data in real time. The addition of blockchain strengthens the system by ensuring data integrity and transparency. Although problems such as technological complexity, data privacy, and cybersecurity threats persist, integrating AI with AIDC technology is a big step towards creating secure and efficient supply chains. Future research should address these difficulties and investigate novel methods to use these technologies to improve supply chain security and management. Table 2 presents a summary of supply chain security and the role of AI integration for automatic identification data capture.

Table 2: The summary of Supply chain security and the role of AI integration for automatic identification data capture.

Authors	Title	Year	Source title	Cited by
Nguyen H.; Scala N.M.; Dehlinger J.	Analysis of Security Behaviors of Supply Chain Professionals	2024	Proceedings of the IISE Annual Conference and Expo 2024	0
Karai Y.; Chroqui R.	Integration of Artificial Intelligence of Things and Blockchain Technologies	2024	Lecture Notes in Networks and Systems	0

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

	for Enhanced Supply Chain Management			
Samayamantri L.S.	Challenges and Prospects of Implementing: AI-Powered Retail and Consumer Packaged Solutions in the Global Supply Chain for Enhanced Well-Being	2024	Artificial Intelligence and Machine Learning for Sustainable Development: Innovations, Challenges, and Applications	0
Shobika G.V.; Chakraborty S.; Krishna V.; Mishra D.N.; Kumar P.	Artificial intelligence in marketing and operations	2023	Artificial Intelligence and Knowledge Processing: Methods and Applications	0
Hruska R.; Svadlenka L.; Jurankova P.	Challenges for automatic identification systems in the supply chain	2019	International Journal of Learning and Change	2
Kelepouris T.; McFarlane D.; Parlikad A.K.	Developing a model for quantifying the quality and value of tracking information on supply chain decisions	2007	Proceedings of the 2007 International Conference on Information Quality, ICIQ 2007	7
Cook S.	Benefits of implementing automatic identification technology to improve the efficiency of the FAA logistics	2005	50th Annual Air Traffic Control Association Conference Proceedings - Fall 2005	0

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

center's supply chain

Having explored the role of AI integration in enabling automatic identification and data capture to enhance supply chain security, the next section will focus on its application in fostering collaborative work environments. Specifically, it will examine how AI-driven insights and shared data empower stakeholders to collectively mitigate risks and strengthen supply chain resilience.

Linkage between Supply Chain security to AI Integration for Collaborative Work

Supply chain security is a complex challenge that necessitates cooperation from all stakeholders to ensure the integrity, transparency, and resilience of supply chain operations. The integration of Artificial Intelligence (AI) into collaborative supply chain management has emerged as a game-changing approach for increasing security while encouraging trust and transparency among partners. AI addresses supply chain security vulnerabilities such as counterfeiting, data breaches, and operational interruptions through timely insights and data-driven decision-making (Ali et al., 2024; Nitsche et al., 2021). Its capacity to support seamless information sharing and develop collaborative partnerships enables organisations to effectively minimise risks while maintaining network security.

AI's ability to improve demand forecasting, inventory management, and resource optimisation demonstrates its importance in boosting collaborative work within supply chains. These skills not only expedite processes but also help to promote sustainability by decreasing waste and minimising environmental effect (Samuels, 2024). For example, AI solutions can detect irregularities in business processes or activities in seconds, reducing the need for human intervention and resulting in cost savings and revenue improvements. In terms of supply chain security, this translates into speedier detection of possible dangers, such as counterfeit items or unauthorised access, allowing for proactive actions. Furthermore, AI builds confidence among supply chain partners by guaranteeing that provided data is accurate, trustworthy, and actionable—an important aspect in preserving network security and accountability.

The evolving nature of supply networks and information systems highlights the need for structured frameworks to guide AI integration in collaborative supply chain management. A five-stage AI collaboration framework has been proposed to help managers assess their organization’s progress in adopting AI (Weisz et al., 2025). This framework emphasizes a progression from basic information sharing to advanced levels of trust and transparency, which are foundational for secure and resilient supply chains. By leveraging AI to facilitate these stages, organizations can build stronger collaborative relationships, ensuring that all partners are aligned in their efforts to combat security threats. Such alignment is particularly crucial in combating counterfeiting and ensuring the authenticity of goods throughout the supply chain.

Despite its benefits, integrating AI into collaborative supply chain management presents challenges that must be addressed to maximize its impact on security. Technical complexity, data privacy concerns, and resistance to change are significant barriers that organizations must overcome (Ali et al., 2024; Al-Alawi et al., 2021). Additionally, the effectiveness of AI-driven collaboration depends on the willingness of supply chain partners to share sensitive data, which may raise concerns about confidentiality and misuse. To address these issues, organizations must adopt robust cybersecurity measures and establish clear governance frameworks that

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

define data-sharing protocols and responsibilities. By doing so, they can create a secure environment that encourages collaboration while safeguarding sensitive information.

Finally, integrating AI into collaborative supply chain management provides a promising avenue to improving supply chain security. AI helps organisations manage vulnerabilities and reduce risks more effectively by encouraging trust, openness, and efficient information sharing. Structured frameworks, such as the five-stage AI collaboration model, offer useful assistance for organisations looking to use AI in collaborative endeavours. However, overcoming technical and organisational difficulties is critical to fully use AI in this environment. Future research should centre on creating scalable solutions that strike a balance between security, collaboration, and innovation, opening the way for more resilient and secure supply chains. Table 3 summarizes key studies on supply chain security with AI integration in collaborative work.

Table 3: The Summary Of Supply Chain Security With AI Integration In Collaborative Work

Authors	Title	Year	Source title	Cited by
Weisz E.; Herold D.M.; Ostern N.K.; Payne R.; Kummer S.	Artificial intelligence (AI) for supply chain collaboration: implications on information sharing and trust	2025	Online Information Review	2
Samuels A.	Examining the integration of artificial intelligence in supply chain management from Industry 4.0 to 6.0: a systematic literature review	2024	Frontiers in Artificial Intelligence	0
Ali A.A.A.; Sharabati A.-A.A.; Alqurashi D.R.;	The impact of artificial intelligence and supply chain collaboration	2024	Uncertain Supply Chain Management	4

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Shkeer A.S.; Allahham M.	on supply chain resilience: Mediating the effects of information sharing			
Al-Alawi L.; Al-Busaidi R.; Ali S.	Applying NIST SP 800-161 in supply chain processes empowered by artificial intelligence	2021	2021 22nd International Arab Conference on Information Technology, ACIT 2021	1
Nitsche A.-M.; Schumann C.-A.; Franczyk B.; Reuther K.	Artificial intelligence inspired supply chain collaboration: A design-science research and system dynamics approach	2021	2021 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2021 - Proceedings	3

Having explored how AI integration fosters collaborative work to enhance supply chain security, the next focus will shift to the role of blockchain technology, specifically Ethereum, in providing decentralized and transparent solutions that further strengthen the integrity and resilience of supply chains.

Linkage between Supply Chain security to Blockchain Technology for Ethereum

Supply chain security is a major challenge in modern logistics, especially as supply chains become more global and sophisticated. Blockchain technology has emerged as a disruptive option for improving supply chain security through transparency, efficiency, and data integrity (Mishra et al., 2022; Zhang et al., 2024). Ethereum distinguishes out among blockchain platforms because of its decentralised architecture and smart contract features, which allow for secure and automated transactions between supply chain actors (Ahamed & Vignesh, 2023). Organisations can use Ethereum's capabilities to ensure that sensitive supply chain data is tamper-proof, transparent, and only available to authorised parties. This feature is especially useful in preventing counterfeiting, ensuring product authenticity, and fostering confidence throughout the supply chain.

Ethereum's contribution to improving supply chain security is mostly driven by its smart contract functionality and decentralised structure. Smart contracts are self-executing agreements written on the Ethereum blockchain that autonomously enforce established rules without the use of middlemen (Ahamed & Vignesh, 2023). This ensures that protocols are

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
followed without exception, lowering the possibility of human error or hostile intervention (Terzi et al., 2019). For instance, in food supply chain management, Ethereum-based smart contracts have been utilized to track items from farm to table, assuring compliance with safety requirements and allowing for real-time transaction verification (Ahamed & Vignesh, 2023). Similarly, Ethereum's decentralized architecture ensures that no single party has complete control of the system, making it highly resistant to data tampering and unauthorized access (Ismail & Reza, 2022). These elements improve the dependability and security of supply chain operations.

Despite its benefits, incorporating Ethereum-based blockchain technology into supply chain management raises a few obstacles that must be solved. Scalability is still a major worry, since Ethereum's existing infrastructure may struggle to handle the massive volume of transactions seen in large-scale supply chains (Zhang et al., 2024). Furthermore, smaller firms may find the expense of establishing and maintaining Ethereum-based systems prohibitively high (Mishra et al., 2022). Security concerns, such as smart contract vulnerabilities and the possibility of malicious attacks, endanger the integrity and confidentiality of supply chain data (Vashishth et al., 2024). To prevent these risks, firms must use strong encryption techniques, rigorously test smart contracts, and build continuous monitoring systems that detect and respond to any threats.

The integration of Ethereum into supply chain security offers a promising pathway to address many of these challenges while enhancing operational efficiency. For instance, Ethereum's ability to facilitate secure and transparent transactions can streamline administrative activities, reduce costs, and improve decision-making processes (Singh et al., 2024). Moreover, Ethereum's interoperability with other technologies, such as the Internet of Things (IoT), enables real-time tracking and verification of goods throughout the supply chain (Singh et al., 2024). This combination not only enhances visibility but also ensures that all stakeholders have access to accurate and up-to-date information, fostering trust and collaboration. By addressing scalability and security concerns, Ethereum can serve as a foundational platform for building resilient and secure supply chain systems.

To summarize, Ethereum-based blockchain technology has considerable potential to improve supply chain security by increasing transparency, efficiency, and data integrity. Its decentralized architecture and smart contract features allow for secure and automated transactions, assuring protocol compliance and lowering the danger of counterfeiting. However, obstacles such as scalability, cost, and security risks must be solved in order to optimize the benefit. Future research should concentrate on establishing scalable and cost-effective solutions that capitalize on Ethereum's capabilities while addressing its limitations. This allows enterprises to construct a more secure, transparent, and efficient supply chain ecosystem. Table 4 summarizes key studies on supply chain security using Ethereum-based blockchain technology.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Table 4: The Summary Of Supply Chain Security Using Ethereum-Based Blockchain Technology

Authors	Title	Year	Source title	Cited by
Vashishth T.K.; Sharma V.; Sharma K.K.; Kumar B.; Chaudhary S.; Panwar R.	Security and privacy challenges in blockchain-based supply chain management: A comprehensive analysis	2024	Achieving Secure and Transparent Supply Chains With Blockchain Technology	3
Singh I.; Singh B.; Rana A.K.	Role and Impact of Blockchain-IoT-Enabled Supply Chain Management Model for Medical Supply	2024	Convergence of Blockchain and Internet of Things in Healthcare	1
Ghodake S.P.; Tidake V.M.; Singh S.; Muniyandy E.; Mohit; Maguluri L.P.; Mesia Dhas J.T.	Enhancing Supply Chain Transparency and Efficiency Through Innovative Blockchain Solutions for Optimal Operations Management	2024	International Journal of Advanced Computer Science and Applications	0
Zhang W.; Di L.; Yan L.; Li D.; Yu W.; Wu J.	When Supply Chain Security Meets Blockchain: Applications and Challenges	2024	Communications in Computer and Information Science	0
Ahamed N.N.; Vignesh R.	A Build and Deploy Ethereum Smart Contract for Food Supply Chain	2023	2023 9th International Conference on Advanced Computing and Communication	5

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

	Management in Truffle - Ganache Framework		Systems, ICACCS 2023	
Vora D.K.; Patel J.H.; Shah D.; Mehta P.	Application of Blockchain in Different Segments of Supply Chain Management	2022	Lecture Notes in Electrical Engineering	1
Mishra D.; Singh P.; Singh N.	Role of blockchain in achieving solutions in ambiguous supply chain operations	2022	Blockchain in a Volatile-Uncertain-Complex-Ambiguous World	5
Ismail S.; Reza H.	Security Challenges of Blockchain-Based Supply Chain Systems	2022	2022 IEEE 13th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2022	9
Smith K.J.; Dhillon G.	Supply Chain Virtualization: Facilitating Agent Trust Utilizing Blockchain Technology	2019	Springer Series in Supply Chain Management	12
Terzi S.; Zacharaki A.; Nizamis A.; Votis K.; Ioannidis D.; Tzovaras D.; Stamelos I.	Transforming the supply-chain management and industry logistics with blockchain smart contracts	2019	ACM International Conference Proceeding Series	19

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Having explored the role of Ethereum in enhancing supply chain security through decentralized smart contracts and transparent transaction records, the next section will focus on Hyperledger Fabric. This permissioned blockchain framework is tailored for enterprise-level supply chain applications, ensuring privacy, scalability, and efficient consensus mechanisms.

Linkage between Supply Chain security to Blockchain Technology for Hyperledger Fabric

Supply chain security is a major challenge in modern logistics, especially as supply chains become more global and sophisticated. Blockchain technology, notably Hyperledger Fabric, has emerged as a game-changing solution for improving supply chain security by tackling critical concerns such information asymmetry, transparency, traceability, and data security (Wang et al., 2023; Ma et al., 2019). Hyperledger Fabric's modular architecture and permissioned blockchain structure make it ideal for supply chain applications that require tamper-proof, traceable, and trustworthy data. This skill is critical for preventing counterfeiting, preserving product authenticity, and sustaining trust across the supply chain.

Hyperledger Fabric's contribution to supply chain security is highlighted by its capacity to provide immutable and tamper-proof methods for tracking information stored on the ledger. For example, in agri-food supply chains, Hyperledger Fabric has been utilized to maintain relationships, authorizations, and exact traceability of agricultural goods across the supply chain (El Hajji et al., 2024). This guarantees that stakeholders have access to accurate and transparent data, lowering the likelihood of counterfeit products entering the supply chain. Furthermore, performance studies have shown that Hyperledger Fabric is feasible and efficient for optimizing supply chain operations, with high stability lowering the likelihood of system vulnerabilities and failures (Liu et al., 2023).

Authentication and verification are key components of supply chain security, and Hyperledger Fabric has been efficiently used to meet these objectives. A multilevel security and authentication application built on Hyperledger Fabric has been proposed to improve transparency, integrity, and traceability in the pharmaceutical supply chain (Sharma & Rohilla, 2024). This application uses a blockchain-based QR code watermarking layer for authentication and verification, assuring that the products are legitimate and untampered. Such technologies not only increase the reliability of supply chain data, but also provide strong procedures for detecting and combating counterfeit items, protecting consumer health and brand reputation.

Despite its benefits, adopting Hyperledger Fabric in supply chain security offers hurdles that must be overcome in order to optimize its impact. Marjanović et al. (2021) identify technical challenges such as interoperability with existing systems, scalability for enormous transaction volumes, and the necessity for significant processing resources. Furthermore, enterprises may encounter adoption challenges due to implementation costs, a lack of knowledge, and aversion to change. To address these issues, organisations must spend in training, infrastructure, and continuous monitoring tools to enable the flawless integration and operation of Hyperledger Fabric-based solutions.

In conclusion, Hyperledger Fabric offers significant potential to enhance supply chain security by ensuring data integrity, improving traceability, and enabling transparent and efficient operations. Its modular architecture, combined with features such as immutability, tamper-proof data storage, and multilevel authentication, makes it a robust platform for combating

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

counterfeiting in supply chains. However, overcoming technical and adoption obstacles is critical to completely reaping the rewards. Future research should focus on establishing scalable and cost-effective solutions that harness Hyperledger Fabric's benefits while minimizing its constraints. By doing so, organizations can create a more secure, transparent, and resilient supply chain ecosystem. Table 5 summarizes key studies on Hyperledger Fabric's role in enhancing supply chain security.

Table 5: The summary of Hyperledger Fabric's role in enhancing Supply Chain Security

Authors	Title	Year	Source title	Cited by
Sharma N.; Rohilla R.	A multilevel authentication-based blockchain powered medicine anti-counterfeiting for reliable IoT supply chain management	2024	Journal of Supercomputing	1
El Hajji M.; Es-saady Y.; Ait Addi M.; Antari J.	Optimization of agrifood supply chains using Hyperledger Fabric blockchain technology	2024	Computers and Electronics in Agriculture	0
Liu J.; Yeoh G.; Gao L.; Gao S.; Ngwenyama O.	Designing a Secure Blockchain-Based Supply Chain Management Framework	2023	Journal of Computer Information Systems	7
Wang J.; Xu H.; Xiao C.; Zhang L.; Zheng Y.	Research and Implementation of the Blockchain-Based Supply Chain Information System	2023	Proceedings of SPIE - The International Society for Optical Engineering	0
Marjanović J.; Dalčeković	Improving Critical Infrastructure Protection by	2021	ACM International Conference	1

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

N.; Sladić G.	Enhancing Software Acquisition Process through Blockchain		Proceeding Series	
Ma C.; Kong X.; Lan Q.; Zhou Z.	The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance	2019	Cybersecurity	85

After discussing the role of Hyperledger Fabric in improving supply chain security through permissioned blockchain frameworks, the following section will focus on the integration of RFID technology, which complements blockchain by allowing for real-time traceability and seamless tracking of products throughout the supply chain.

Linkage between Supply Chain security to RFID Technology for Traceability

Supply chain security is a major challenge in modern logistics, especially as supply chains become more global and sophisticated. Radio Frequency Identification (RFID) technology improves supply chain security by offering traceability, which protects product authenticity and integrity throughout its existence. RFID technology employs radio waves to automatically identify items, delivering real-time information about products as they move through the supply chain (He et al., 2008; Zhu et al., 2012). This feature enables enterprises to follow goods from manufacturing to delivery, lowering the risk of counterfeit products entering the supply chain and maintaining regulatory compliance. By integrating RFID with systems like the EPCglobal Network, stakeholders can share standardized information about tracked items, fostering transparency and trust across the supply chain (He et al., 2008).

RFID technology enhances traceability by enabling the automated capture and sharing of data at various checkpoints in the supply chain. For instance, RFID tags can be scanned at different stages, updating the product's status in real time and ensuring that stakeholders have access to accurate and up-to-date information (Tudora et al., 2011). This level of visibility not only improves inventory management and operational efficiency but also strengthens supply chain security by making it easier to identify and address discrepancies or irregularities (Zhu et al., 2012). Furthermore, RFID tags can be integrated with databases and operational systems to trace resources and emissions, contributing to sustainability efforts while maintaining accountability across the supply chain (Junkkari & Sirkka, 2011).

The use of RFID technology in supply chains provides major competitive advantages by increasing transparency and traceability. In industries like food and pharmaceuticals, where product safety and authenticity are critical, RFID-based traceability solutions ensure that items fulfill quality standards and regulatory requirements. RFID tags, for example, can retain precise information about a product's origin, production process, and transit conditions, enabling

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

stakeholders to verify its legitimacy and safety. This skill is very useful in combatting counterfeiting and maintaining consumer trust in the products they buy.

Despite its benefits, the implementation of RFID technology for traceability presents challenges, particularly concerning privacy and security. RFID tags' ability to track and trace products raises concerns about unauthorized access to sensitive data, necessitating robust security mechanisms to protect against potential threats (Luo et al., 2006). Experimental analyses of RFID security protocols highlight the importance of encryption and authentication measures to safeguard tag data and prevent misuse (Luo et al., 2006). Addressing these challenges is crucial to ensuring that RFID technology enhances supply chain security without compromising privacy or creating vulnerabilities that could be exploited by malicious actors.

To summarize, RFID technology is an effective technique for improving supply chain security through increased traceability. RFID automates product identification and tracking, allowing for real-time visibility and accountability, lowering the danger of counterfeit goods and maintaining regulatory compliance. However, addressing privacy and security concerns is critical to effectively leveraging RFID technology in supply chain management. Future research should concentrate on creating scalable and secure solutions that capitalize on RFID's capabilities while minimizing its drawbacks, opening the way for more transparent and resilient supply chains. Table 6 summarizes key studies on using RFID technology to provide traceability in improving supply chain security.

Table 6: The Summary Of RFID Technology To Provide Traceability Element In Improving Supply Chain Security.

Authors	Title	Year	Source title	Cited by
Zhu X.; Mukhopadhyay S.K.; Kurata H.	A review of RFID technology and its managerial applications in different industries	2012	Journal of Engineering and Technology Management - JET-M	328
Junkkari M.; Sirkka A.	Using RFID for tracing cumulated resources and emissions in supply chain	2011	International Journal of Ad Hoc and Ubiquitous Computing	4
Tudora E.; Alexandru A.; Ianculescu M.	Using radio frequency identification technology in supply chain management	2011	Recent Advances in Applied and Biomedical Informatics and Computational	1

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

			Engineering in Systems Applications - AIC'11, BEBI'11	
He W.; Zhang N.; Tan P.S.; Lee E.W.; Li T.Y.; Lim T.L.	A secure RFID-based track and trace solution in supply chains	2008	IEEE International Conference on Industrial Informatics (INDIN)	18
Luo Z.; Chan T.; Li J.S.; Wong E.; Cheung W.; Ng V.; Fok W.	Experimental analysis of an RFID security protocol	2006	Proceedings - IEEE International Conference on e-Business Engineering, ICEBE 2006	8
Clarson C.	EU food chain traceability rules - Headache or golden opportunity?	2005	Food Australia	0
Macmillan-Davies C.; Squires G.; Greene A.	Markets. Supply chain. Toward a transparency of the supply chain; [Marchés. Supply chain. Vers une transparence de la chaîne logistique]	2005	Cartonnages Emballages Modernes	0

While RFID technology's role in enhancing traceability provides a foundation for real-time tracking and transparency in supply chains, its application in prevention systems further strengthens security by enabling proactive measures to detect and mitigate risks before they escalate.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Linkage between Supply Chain security to RFID Technology for Prevention Systems

Supply chain security is an important consideration in modern logistics, especially as supply chains become more international and interconnected. Radio Frequency Identification (RFID) technology is critical to improving supply chain security because it allows preventative systems to detect and mitigate hazards such as counterfeiting, theft, and unauthorized access. RFID technology enables effective data indexing and retrieval across various participants, permitting real-time product tracking and monitoring throughout the supply chain (Qi et al., 2016; Pal, 2021). However, implementing RFID technology raises security and privacy problems, demanding strong safeguards to maintain the integrity and confidentiality of sensitive supply chain data. Addressing these vulnerabilities is critical to fully utilize RFID's potential as a preventative mechanism.

To address the security challenges associated with RFID technology, researchers have proposed various measures to enhance its reliability in supply chain prevention systems. For instance, dual security modes have been designed to balance security and efficiency in RFID-tagged supply chains (Cai et al., 2010; Cai et al., 2009). These modes ensure that RFID systems can operate securely without compromising performance, making them suitable for large-scale applications. Additionally, lightweight authentication protocols have been developed to protect RFID-assisted supply chain management systems from unauthorized access and cyber threats (Tariq et al., 2024). Such innovations not only improve the security of RFID systems but also make them more adaptable to the dynamic needs of modern supply chains, ensuring that prevention mechanisms remain effective and scalable.

RFID-enabled prevention systems allow for product tracking and detection at various stages of the supply chain, lowering the danger of counterfeit goods entering the system. RFID tags, for example, can be scanned at checkpoints to ensure product authenticity and compliance with quality and regulatory criteria (Lian & Hu, 2014). However, the usage of RFID technology creates concerns regarding privacy and information flow, especially when sensitive data is exchanged with various parties. To solve this, on-demand access control systems have been proposed to govern information sharing in RFID-enabled supply chains, ensuring that only authorized parties have access to important data (Du et al., 2008).

Despite its benefits, implementing RFID technology for prevention systems presents challenges that must be addressed to maximize its impact. Technical complexities, such as interoperability issues and the need for significant computational resources, can hinder the seamless integration of RFID systems into existing supply chain frameworks (Srivastava, 2010). Moreover, the cost of deploying secure RFID solutions may pose a barrier for smaller organizations, requiring innovative approaches to reduce implementation costs while maintaining high security standards (Ray et al., 2013). Addressing these challenges is crucial to ensuring that RFID technology can serve as a reliable tool for preventing security threats in supply chains.

Finally, RFID technology plays an important role in improving supply chain security by implementing risk detection, tracking, and mitigation systems. RFID ensures product authenticity and safety across the supply chain by allowing for real-time monitoring and verification. However, addressing security and privacy concerns is critical to maximizing its potential. Future research should concentrate on establishing scalable and cost-effective systems that capitalize on RFID's benefits while addressing its limitations. This allows

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

enterprises to build a more secure, transparent, and resilient supply chain ecosystem. Table 7 summarizes key studies on using RFID technology for prevention systems to increase supply chain security.

Table 7: The Summary Of Using RFID Technology For Prevention System To Increase Supply Chain Security.

Authors	Title	Year	Source title	Cited by
Tariq T.; Kuo W.-C.; Mahmood K.; Shamshad S.; Das A.K.; Alenazi M.J.F.	A Lightweight Authentication Protocol for RFID-assisted Supply Chain Management System	2024	IEEE Internet of Things Journal	0
Pal K.	Applications of radio frequency identification technology and security issues in supply chain management	2021	Handbook of Research on Recent Perspectives on Management, International Trade, and Logistics	0
Qi S.; Zheng Y.; Li M.; Lu L.; Liu Y.	Secure and Private RFID-Enabled Third-Party Supply Chain Systems	2016	IEEE Transactions on Computers	25
Lian X.; Hu C.-S.	Application of RFID technology in agricultural byproduct logistics and food security supervising	2014	Proceedings - 2014 5th International Conference on Intelligent Systems Design and Engineering Applications, ISDEA 2014	2
Ray B.R.; Chowdhury M.; Abawajy J.	Critical analysis and comparative study of security for networked RFID systems	2013	SNPD 2013 - 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and	15

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

			Parallel/Distributed Computing	
Mukherjee S.; Hasan M.; Chowdhury B.; Chowdhury M.	Security of RFID systems - A hybrid approach	2011	Proceedings - 2011 12th ACIS International Conference on Software Engineering, Artificial Intelligence Networking and Parallel Distributed Computing, SNPD 2011	0
Srivastava B.	Critical management issues for implementing RFID in supply chain management	2010	International Journal of Manufacturing Technology and Management	21
Cai S.; Li Y.; Li T.; Deng R.H.; Yao H.	Achieving high security and efficiency in RFID-tagged supply chains	2010	International Journal of Applied Cryptography	7
Cai S.; Li T.; Li Y.; Deng R.H.	Ensuring dual security modes in rfid-enabled supply chain systems	2009	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	3
Du T.C.; Cheung W.; Chu S.-C.	Designing privacy and security protection in RFID-enabled supply chain	2008	Proceedings of the International Conference on Electronic Business (ICEB)	0

Building on the insights and findings discussed in the results and discussion section, the next section synthesizes these outcomes to highlight the transformative potential of integrating Blockchain, AI, and RFID technologies in combating counterfeiting. This synthesis also addresses the challenges and proposes future directions for research and implementation, paving the way for more secure and resilient supply chains.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007

Conclusion

The integration of Blockchain, AI, and RFID technologies offers a transformative approach to combating counterfeiting in supply chain management. Blockchain provides decentralization, immutability, and transparency, ensuring that all transactions are securely recorded and visible to stakeholders (Pandey & Singh, 2024; Kamble & Joshi, 2024). RFID technology complements this by enabling real-time tracking and physical-layer authentication, making it significantly harder for counterfeiters to replicate or tamper with products (Wang et al., 2023; Islam et al., 2022). AI further enhances the system by analyzing patterns, detecting anomalies, and automating verification processes, thereby reducing the need for manual checks and increasing operational efficiency (Banu et al., 2024). Together, these technologies create a multi-layered defense mechanism that ensures both digital and physical security, addressing the complex challenges of modern supply chains.

The practical implications of this integrated framework are profound. By leveraging Blockchain's transparency, RFID's real-time tracking capabilities, and AI's analytical power, organizations can achieve end-to-end traceability and accountability in their supply chains. For instance, IoT-based secure medicine supply chains and electronic component authentication systems have demonstrated the effectiveness of these technologies in real-world applications (Chinchmalatpure et al., 2024; Lobachev et al., 2022). Such implementations not only reduce the risk of counterfeit products but also streamline administrative processes, enhance compliance with regulatory standards, and build trust among stakeholders. This makes the integration of Blockchain, AI, and RFID particularly valuable for industries such as pharmaceuticals, electronics, and luxury goods, where counterfeiting poses significant risks to consumer safety and brand reputation.

Despite its promise, the adoption of these technologies is not without challenges. Technical complexities, such as interoperability, scalability, and the need for significant computational resources, remain significant barriers (Budyal et al., 2024; Sidorov et al., 2019). Additionally, the cost of implementation and the lack of expertise in deploying these technologies may hinder widespread adoption, particularly for smaller organizations (Kamble & Joshi, 2024). Furthermore, ensuring secure communication between RFID tags and Blockchain nodes requires robust ultra-lightweight mutual authentication protocols, which are still under development (Sidorov et al., 2019). Addressing these challenges is crucial to realizing the full potential of this integrated framework.

Future research should focus on overcoming these limits while also exploring new avenues for innovation. Key areas of investigation include developing scalable solutions capable of handling large amounts of data, designing cost-effective methods for integrating these technologies into existing systems, and developing standardized regulatory frameworks to facilitate industry adoption (Alqarni et al., 2023). Furthermore, investigating the function of smart contracts in automating complicated supply chain operations such as payments and compliance checks may improve efficiency and transparency (Alqarni et al., 2023). Industry-specific case studies, notably in healthcare, agriculture, and manufacturing, could offer more insight into customizing these solutions to specific difficulties.

To summarize, the combination of Blockchain, AI, and RFID technologies provides a comprehensive and robust solution to prevent counterfeiting in supply chain management. This architecture has the ability to change modern supply chains by ensuring high security,

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
transparency, and efficiency, while also protecting the authenticity and safety of commodities from manufacture to delivery. However, addressing technical, financial, and regulatory barriers is critical to wider adoption. Future research and industry collaboration will be critical in improving these technologies and realizing their full promise to create more robust, transparent, and trustworthy supply chains.

Acknowledgements
The authors would like to express their sincere gratitude to the Kedah State Research Committee, UiTM Kedah Branch, for the generous funding provided under the Tabung Penyelidikan Am. This support was crucial in facilitating the research and ensuring the successful publication of this article.

References
Ahamed, N. N., & Vignesh, R. (2023). A build and deploy Ethereum smart contract for food supply chain management in Truffle-Ganache framework . 2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023.

Ali, A. A. A., Sharabati, A.-A. A., Alqurashi, D. R., ..., Allahham, M. (2024). The impact of artificial intelligence and supply chain collaboration on supply chain resilience: Mediating the effects of information sharing. Uncertain Supply Chain Management.

Al-Alawi, L., Al-Busaidi, R., & Ali, S. (2021). Applying NIST SP 800-161 in supply chain processes empowered by artificial intelligence. 2021 22nd International Arab Conference on Information Technology, ACIT 2021.

Alqarni, M. A., Alkatheiri, M. S., Chauhdary, S. H., & Saleem, S. (2023). Use of blockchain-based smart contracts in logistics and supply chains. Electronics (Switzerland).

Banu, E. A., Priyanka, R., Thiruramanathan, P., ..., Vinoth, K. (2024). Robust AI-enabled electronic components authentication and anti-counterfeiting. Proceedings of 9th International Conference on Science, Technology, Engineering and Mathematics: The Role of Emerging Technologies in Digital Transformation, ICONSTEM 2024.

Cai, S., Li, T., Li, Y., & Deng, R. H. (2009). Ensuring dual security modes in RFID-enabled supply chain systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).

Cai, S., Li, Y., Li, T., ..., Yao, H. (2010). Achieving high security and efficiency in RFID-tagged supply chains. International Journal of Applied Cryptography.

Chinchmalatpure, S., Pala, A., Waghmare, A., ..., Diwnale, T. (2024). IoT-based secure medicine supply chain using blockchain technology. 2024 8th International Conference on Computing, Communication, Control and Automation, ICCUBEA 2024.

Clarson, C. (2005). EU food chain traceability rules - Headache or golden opportunity? Food Australia.

Cook, S. (2005). Benefits of implementing automatic identification technology to improve the efficiency of the FAA logistics center's supply chain. 50th Annual Air Traffic Control Association Conference Proceedings - Fall 2005.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Du, T. C., Cheung, W., & Chu, S.-C. (2008). Designing privacy and security protection in RFID-enabled supply chain. Proceedings of the International Conference on Electronic Business (ICEB).

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
El Hajji, M., Es-saady, Y., Ait Addi, M., & Antari, J. (2024). Optimization of agrifood supply chains using Hyperledger Fabric blockchain technology. Computers and Electronics in Agriculture.

Ghodake, S. P., Tidake, V. M., Singh, S., ..., Mesia Dhas, J. T. (2024). Enhancing supply chain transparency and efficiency through innovative blockchain solutions for optimal operations management. International Journal of Advanced Computer Science and Applications.

He, W., Zhang, N., Tan, P. S., ..., Lim, T. L. (2008). A secure RFID-based track and trace solution in supply chains. IEEE International Conference on Industrial Informatics (INDIN).

Hruska, R., Svadlenka, L., & Jurankova, P. (2019). Challenges for automatic identification systems in the supply chain. International Journal of Learning and Change.

Ismail, S., & Reza, H. (2022). Security challenges of blockchain-based supply chain systems. 2022 IEEE 13th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2022.

Islam, M. D., Shen, H., & Badsha, S. (2022). Integrating blockchain into supply chain safeguarded by PUF-enabled RFID. Internet of Things (Netherlands).

Junkkari, M., & Sirkka, A. (2011). Using RFID for tracing cumulated resources and emissions in supply chain. International Journal of Ad Hoc and Ubiquitous Computing.

Kamble, V. M., & Joshi, R. B. (2024). Empowering consumers through blockchain product authentication. 15th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2024.

Karai, Y., & Chroqui, R. (2024). Integration of artificial intelligence of things and blockchain technologies for enhanced supply chain management. Lecture Notes in Networks and Systems.

Kelepouris, T., McFarlane, D., & Parlikad, A. K. (2007). Developing a model for quantifying the quality and value of tracking information on supply chain decisions. Proceedings of the 2007 International Conference on Information Quality, ICIQ 2007.

Lian, X., & Hu, C.-S. (2014). Application of RFID technology in agricultural byproduct logistics and food security supervising. Proceedings - 2014 5th International Conference on Intelligent Systems Design and Engineering Applications, ISDEA 2014.

Liu, J., Yeoh, G., Gao, L., ..., Ngwenyama, O. (2023). Designing a secure blockchain-based supply chain management framework. Journal of Computer Information Systems.

Lobachev, E., Mahmoud, M. N., & Patooghy, A. (2022). Blockchain-based smart supply chain management. Proceedings - 2022 9th International Conference on Dependable Systems and Their Applications, DSA 2022.

Luo, Z., Chan, T., Li, J. S., ..., Fok, W. (2006). Experimental analysis of an RFID security protocol. Proceedings - IEEE International Conference on e-Business Engineering, ICEBE 2006.

Ma, C., Kong, X., Lan, Q., & Zhou, Z. (2019). The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance. Cybersecurity.

Macmillan-Davies, C., Squires, G., & Greene, A. (2005). Markets. Supply chain. Toward a transparency of the supply chain. Cartonnages Emballages Modernes.

Mandal, R., Siriporam, R. N., Gopika, G. S., ..., Supriya, S. (2024). Spotting simulated commodity welding metamask technology. 2nd International Conference on Artificial Intelligence and Machine Learning Applications: Healthcare and Internet of Things, AIMLA 2024.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
Marjanović, J., Dalčeković, N., & Sladić, G. (2021). Improving critical infrastructure protection by enhancing software acquisition process through blockchain. ACM International Conference Proceeding Series.

Mishra, D., Singh, P., & Singh, N. (2022). Role of blockchain in achieving solutions in ambiguous supply chain operations. Blockchain in a Volatile-Uncertain-Complex-Ambiguous World.

Nguyen, H., Scala, N. M., & Dehlinger, J. (2024). Analysis of security behaviors of supply chain professionals. Proceedings of the IISE Annual Conference and Expo 2024.

Nitsche, A.-M., Schumann, C.-A., Franczyk, B., & Reuther, K. (2021). Artificial intelligence inspired supply chain collaboration: A design-science research and system dynamics approach. 2021 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2021 - Proceedings.

Pal, K. (2021). Applications of radio frequency identification technology and security issues in supply chain management. Handbook of Research on Recent Perspectives on Management, International Trade, and Logistics.

Pandey, S., & Singh, A. K. (2024). Blockchain-based fake product detection system: Enhancing supply chain transparency. 1st International Conference on Pioneering Developments in Computer Science and Digital Technologies, IC2SDT 2024 - Proceedings.

Qi, S., Zheng, Y., Li, M., ..., Liu, Y. (2016). Secure and private RFID-enabled third-party supply chain systems. IEEE Transactions on Computers.

Ray, B. R., Chowdhury, M., & Abawajy, J. (2013). Critical analysis and comparative study of security for networked RFID systems. SNPD 2013 - 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing.

Samayamantri, L. S. (2024). Challenges and prospects of implementing: AI-powered retail and consumer packaged solutions in the global supply chain for enhanced well-being. Artificial Intelligence and Machine Learning for Sustainable Development: Innovations, Challenges, and Applications.

Samuels, A. (2024). Examining the integration of artificial intelligence in supply chain management from Industry 4.0 to 6.0: A systematic literature review. Frontiers in Artificial Intelligence.

Sidorov, M., Ong, M. T., Sridharan, R. V., ..., Khor, J. H. (2019). Ultralightweight mutual authentication RFID protocol for blockchain-enabled supply chains. IEEE Access.

Singh, I., Singh, B., & Rana, A. K. (2024). Role and impact of blockchain-IoT-enabled supply chain management model for medical supply. Convergence of Blockchain and Internet of Things in Healthcare.

Smith, K. J., & Dhillon, G. (2019). Supply chain virtualization: Facilitating agent trust utilizing blockchain technology. Springer Series in Supply Chain Management.

Srivastava, B. (2010). Critical management issues for implementing RFID in supply chain management. International Journal of Manufacturing Technology and Management.

Tariq, T., Kuo, W.-C., Mahmood, K., ..., Alenazi, M. J. F. (2024). A lightweight authentication protocol for RFID-assisted supply chain management system. IEEE Internet of Things Journal.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18 (7), 509–533.

Tudora, E., Alexandru, A., & Ianculescu, M. (2011). Using radio frequency identification technology in supply chain management. Recent Advances in Applied and Biomedical

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 87-118
DOI: 10.35631/JISTM.1038007
Informatics and Computational Engineering in Systems Applications - AIC'11, BEBI'11.

Vashishth, T. K., Sharma, V., Sharma, K. K., ..., Panwar, R. (2024). Security and privacy challenges in blockchain-based supply chain management: A comprehensive analysis. Achieving Secure and Transparent Supply Chains With Blockchain Technology.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540

Wang, G., Shi, S., Wang, M., ..., Zhao, J. (2023). RF-Chain: Decentralized, credible, and counterfeit-proof supply chain management with commodity RFIDs. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.

Wang, J., Xu, H., Xiao, C., ..., Zheng, Y. (2023). Research and implementation of the blockchain-based supply chain information system. Proceedings of SPIE - The International Society for Optical Engineering.

Weisz, E., Herold, D. M., Ostern, N. K., ..., Kummer, S. (2025). Artificial intelligence (AI) for supply chain collaboration: Implications on information sharing and trust. Online Information Review.

William H. DeLone, Ephraim R. McLean, (1992) Information Systems Success: The Quest for the Dependent Variable. Information Systems Research 3(1):60-95.

Zhang, W., Di, L., Yan, L., ..., Wu, J. (2024). When supply chain security meets blockchain: Applications and challenges. Communications in Computer and Information Science.

Zhu, X., Mukhopadhyay, S. K., & Kurata, H. (2012). A review of RFID technology and its managerial applications in different industries. Journal of Engineering and Technology Management - JET-M.