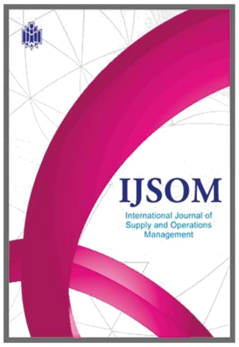
International Journal of Supply and Operations Management

IJSOM

2024, Volume xx, Issue xx, pp. xx-xx
ISSN-Print: 2383-1359
ISSN-Online: 2383-2525
www.ijsom.com



A Survey on Supply Chain Management: Exploring Physical and Cyber Security Challenges, Threats, Critical Applications, and Innovative Technologies

Rashid Hussain Khokhar [a*], Windhya Rankothge [c], Leila Rashidi [b], Hesamodin Mohammadian [c], Ali Ghorbani [c], Brian Frei [d], Shawn Ellis [d] and Iago Freitas [d]

[a] *Algoma University, Sault Ste. Marie, Canada*
[b] *Huawei Technologies Canada Co., Ltd*
[c] *Canadian Institute for Cybersecurity, University of New Brunswick, Fredericton, Canada*
[d] *ADGA Group Consultants Inc., Ottawa, Canada*

Abstract

Supply chain cybersecurity has become a critical concern for organizations due to the increasing frequency of cyber threats that endanger sensitive information, disrupt operations, and cause financial harm. This survey article presents the outcomes of a comprehensive study aimed at deepening our understanding of the challenges and best practices in supply chain cybersecurity. It provides a comprehensive review of critical applications that are susceptible to cyber threats across various sectors of the supply chain. The literature review identifies two distinct categories of approaches utilized to secure the supply chain: traditional and innovative methods. Both categories are extensively examined, providing valuable insights into the current state of supply chain cybersecurity. The findings of this study serve as a valuable resource for organizations seeking to enhance their cybersecurity strategies and fortify their resilience against evolving cyber threats. Furthermore, this research contributes to the knowledge base of supply chain management by facilitating the development of robust and efficient supply chain cybersecurity frameworks. By understanding vulnerabilities and best practices, organizations can proactively tackle cybersecurity challenges and safeguard their supply chains effectively. This survey article empowers organizations with practical insights and guidance to enhance their cybersecurity posture in the dynamic landscape of supply chain operations.

Keywords: Supply Chain Management; Cybersecurity; Physical Security; Blockchain Technology; Artificial Intelligence; Physically Unclonable Function.

1. Introduction

Product manufacturing and its delivery to an end user is a complicated process that involves several independent stakeholders, such as raw material producers, product assemblers, wholesalers, retailer merchants and transportation companies. This is generally known as a supply chain La Londe & Masters (1994), which is shown in Figure 1. It usually involves many organizations and individuals upstream for provisioning and downstream for distribution, along with the flows of products, services, and information from the supplier to the customer Christopher (1992); Mentzer et al. (2001). Based on the literature, *Supply Chain Management* (*SCM*) is a systematic approach that views the entire supply and manages the total flow, starting from the provision of raw material by the supplier and ending at the product

*Corresponding author email address: rashid.khokhar@algomau.ca

DOI:

received by the customer. The objective of SCM is to synchronize and converge intra-firm and inter-firm operations leading to customer satisfaction with the product Cooper & Ellram (1993); Monczka et al. (1998). A sustainable SCM process is vital for any organization to continue their business despite of any unfavorable and unexpected situations such as disasters, pandemics and economic or political crisis Fiorini & Jabbour (2017).

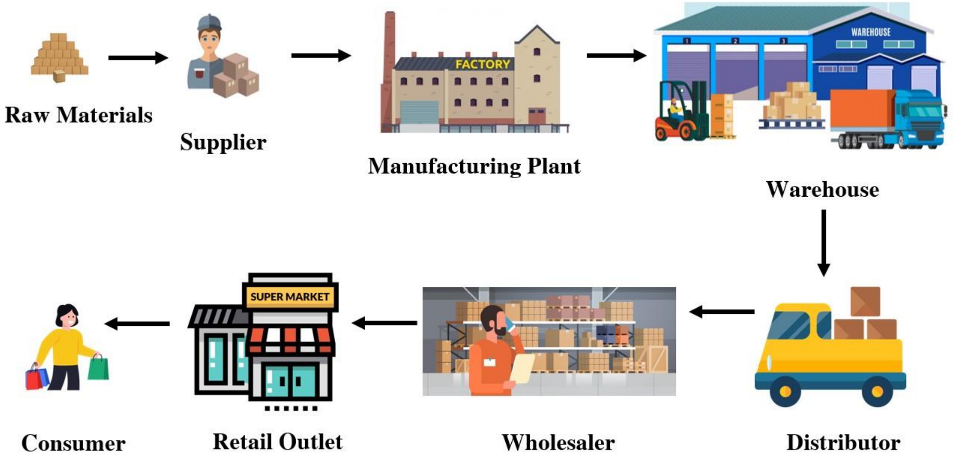


Figure 1. General overview of the supply chain

With the modern-day markets, supply chains are experiencing digital transformations as the stakeholders of supply chains span across multiple geographical areas and collaborate through digital mediums, such as digitized SCM platforms, supply chain software applications and cloud networks Hammi et al. (2023). As the entire supply chain process involves critical information, such as materials, suppliers, productions and customers, organizations use digital storage to store and analyze these pieces of critical information. Often they share information with collaborators and other stakeholders through networks, mainly through internet-based approaches. Furthermore, organizations use different software developed by third-party organizations for the SCM process Hammi & Zeadally (2023). Therefore, SCM plays a vital role in ensuring the smooth functioning of the digitized supply chain, especially considering the security aspects Hassija et al. (2020). Security breaches can happen at any point in the supply chain, in raw materials, suppliers, production, distribution, customer or marketplace Iro (2021). Traditionally, supply chain security mainly focused on physical security related to products. However, with the digitization of supply chains, cyber threats have become a major concern, as they exploit vulnerabilities of platforms, software, and digital services related to the entire supply chain Hassija et al. (2020).

Generally, any incident that can harm an information system through different actions, such as unauthorized access, unauthorized disclosure, unauthorized modification and denial of service, is known as a cyber-threat Booz-Allen & Hamilton (2004). According to the European Union Agency for Cybersecurity (ENISA) ENI (2022) (previously known as European Network and Information Security Agency), cyber threats have increased recently in terms of numbers, vectors and impact. According to statistics derived by ENISA from studying 24 attacks on supply chains that occurred within 18 months starting from January 2020, several industries, such as transport, construction, education, energy and others, have been affected by cyber threats ENI (2021b). This is mainly because of the rapid digitization of information systems, the COVID-19 pandemic and remote working conditions Wong et al. (2022). According to ENISA, various cybercrime groups have emerged to offer" Cybercrime-as-a-Service," and this ecosystem of cybercrime is worldwide in scope, with cybercriminals operating from all over the world. They offer services, including cybercrimes like ransomware, phishing kits, and DDoS attack tools, among others.

ENISA has identified eight threat groups, including ransomware, malware, social engineering, threats against data, denial of service, internet threats, disinformation, and supply chain attacks ENI (2022). As supply chain threats have been identified as one of the main cyber threats, securing the supply chain is very crucial for the smooth functioning of any supply chain. By compromising a single supplier, attackers can get access to its distribution systems and convert any application that is sold, any software update that is pushed, and any physical equipment that is shipped to customers into destructive malware, such as a Trojan horse. According to the annual survey conducted by BlueVoyant Blu (2021), an average number of supply chain cyber threats saw a 37% increase from 2020 to 2021. Furthermore, 97% of organizations that participated in the survey have been impacted by a cybersecurity threat that targeted their supply chain. The study was carried out by an independent survey organization (Opinion Matters). They collected the data from 1,200 Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and Chief Procurement Officers (CPOs) in organizations that have over 1000 employees and represent different industries, such as business services, financial services, healthcare and pharmaceutical, manufacturing, utilities and energy, and defence. It covered six countries, including the USA, Canada, Germany, Netherlands, United Kingdom, and Singapore.

Recently in March 2022, Toyota company of Japan had to pause the production of 14 branches for a day because of a cyber-attack on one of the company's suppliers: Kojima Industries Corp, which supplied plastic parts and electronic components Green (2022). Toyota company had to suffer a production loss of 13,000 vehicles. SolarWinds in 2020 and Kayesa in 2021 attacks ENI (2021b) are considered the biggest supply chain attacks in the recent past that exploited software vulnerabilities of the supply chains. Around 18,000 organizations and government entities that were using SolarWinds's Orion software were infected. Their sensitive information related to user IDs, passwords, financial records and source code was exposed to the attackers. In another case, around 1500 companies that were using Kaseya VSA software got affected. In this attack, cybercriminals demanded a ransom of 70 million dollars from Kaseya.

There are several ways to compromise supply chains, such as malware infection, social engineering, software or configuration vulnerabilities, and brute force attacks. A supply chain cyber threat analysis by ENISA ENI (2021b) found that 62% of supply chain attacks used malware infections as their attack method, particularly when they targeted suppliers' codes. Of the attacks, 58% were directed at obtaining customer information, including personal information and intellectual property, while 16% were directed at obtaining information about important individuals. They studied 24 major supply chain attacks that were reported from January 2020 to early July 2021 for their analysis.

Advanced Persistent Threat (APT) actors are developing complex and more devastating supply chain attacks. According to ENISA ENI (2021b), more than 50% of the supply chain intrusions that were looked into involved well-known cybercrime organizations, such as APT29, APT41, Thallium APT, UNC2546, and Lazarus APT. The report reveals that, for 66% of the attacks that were analyzed, affected suppliers were unaware of how they had been infiltrated, which is a frustrating position given that supply chain attacks are becoming more complex ENI (2021b).

1.1. Related Works

In this section, we review the previous surveys which are related to the security of supply chains. In 2013, Urciuoli et al. Urciuoli et al. (2013) surveyed on cybercrimes, where supply chain crimes were considered to be independent. Different scenarios are also presented to show how cybercrimes can be used to develop other crimes in the supply chain, such as pharma sabotage, arms smuggling, and cargo theft. Despite the merits of the study presented in Urciuoli's paper Urciuoli et al. (2013), it is important to note that the survey was not extensive and did not delve into the history of cybercrimes on supply chains over previous decades. Note that cyber threats in supply chains are not novel. For example, the IT sector was hit hard even more than 10 years ago Boyson (2014). It is crucial to have a comprehensive understanding of the evolution of cyber threats in order to effectively combat them in the present day.

In 2019, Ghadge et al. Ghadge et al. (2019) reviewed the management of cyber risk in the supply chain. They identified five different kinds of cyber risks, including physical threats, breakdown, direct attacks, indirect attacks, and insider threats: (1) *physical threats* refer to the cyber risks which are derived by damaging or theft of physical assets in supply chain networks. For example, a natural disaster that disrupts the functioning of a server would create problems in cyber supply chain networks. (2) *breakdown* refers to cyber risks derived by breaking down some resources. For example, an outdated firewall can give access to production lines Khursheed et al. (2016). (3) *direct attacks* are those attacks in which attacking is done directly over the target, including hacking attacks, denial of service or password sniffing. (4) *indirect attacks* in which attackers design baits to access the target system if employees fall into the trap. These attacks can be conducted using viruses, Trojans, worms, software and hardware, and counterfeit product. For example, bait can be visiting a website or downloading software which seems trustworthy. (5) *Insider threats* are because of a company's internal employees who misuse their access to systems and facilities. Furthermore, in the same study Ghadge et al. (2019), authors focus on Points of Penetration (PoP), propagation levels, consequences, and measures to mitigate risks. They discussed technical points of penetration, human points of penetration, and physical points of penetration for cyber-attacks on supply chains. An example of a technical point of penetration could be obsolete firewalls which enabled attackers to gain remote access to production lines in 2016 Ranathunga et al. (2016). Some researchers believe that future cyber-attacks are through a human point of penetration rather than a technical domain. Physical PoP refers to physical infrastructures, such as machines and buildings, which are always vulnerable to physical attacks that impact cyber systems.

In 2021, Cheung et al. Cheung et al. (2021) performed an extensive survey on measures that can be employed for the cybersecurity of logistics and supply chains. They highlighted the topics which have not received enough attention from the research community, such as real cybersecurity data and the cybersecurity of logistics as a key part of the supply chain. Selecting over 100 papers, Cheung et al. presented a descriptive analysis of papers in terms of the number of articles published per year and the distribution of articles based on the research methodology and design. In Cheung et al. (2021), the articles have been mapped to one of precautionary, real-time recovery, and aftermath planning stages based on the nature of measures proposed to mitigate cyber-attacks. The precautionary planning stage includes access control, risk identification, data protection, etc. while the real-time recovery planning stage corresponds to component recovery and isolation, real-time monitoring, supply chain partner interaction, and task force. Moreover, behavior analysis and feedback, data backups, and recovery plan procedures are three examples of measures taken in the aftermath planning stage.

In addition to the above surveys, some surveys target using specific technologies for the security management of supply chains. In 2021, Asante et al. Asante et al. (2021) conducted a literature review on over one hundred articles about securing supply chains with Distributed Ledger Technologies (DLTs). They analyzed the extent to which DLTs are used and their efficacy in securing the supply chain. Provenance, encryption, authentication, immutability, transparency, consensus, and smart contract are some capabilities of DLTs which improve the integrity of the supply chain. On the other hand, distribution and decentralization increase availability. Moreover, DLTs provide data privacy, which results in confidentiality.

1.2. Contributions

Although a set of measures are introduced in Ghadge et al. (2019); Cheung et al. (2021) to mitigate the cyber risks, the techniques and technologies which can be leveraged for cybersecurity purposes have not been discussed in depth. In order to help researchers and industries enhance the cybersecurity of the supply chain, a big picture of existing methods and technologies and the benefits and disadvantages of each one is of utmost importance. This matter is considered in our study, and we categorize the approaches presented in the literature into traditional and innovative methods in supply chain security.

We mainly considered papers published in academic journals and conferences, particularly those published in 2015 and onwards, and articles published by high-tech companies active in cybersecurity. We also analyzed the reports and news from the mainstream. Table 1 represents a summary of the contributions of the research papers reviewed in this study. The contribution of this survey is outlined below.

- We present an overview of supply chain threats, considering physical threats as well as cyber threats. We explore cyber threats that target data, networks, hardware and software of supply chain management systems.

- We provide an extensive review of critical applications which are vulnerable to cyber threats on the supply chain. We review different sectors, namely health, energy, cyberphysical systems, agriculture, logistics, and IT.

- We study literature on the traditional approaches such as QR-code and RFID tags used for the physical security of the supply chain, particularly centralized supply chain processes.

- We review innovative technologies, such as blockchain, artificial intelligence, machine learning, and physically unclonable functions and their applications in supply chains. These emerging technologies are capable of enhancing both the security and efficiency of supply chains.

Table 1. List of academic papers used in this survey with their contribution

Target	Ref.	Contribution
Threats and Attacks	ENI (2021c)	Mapping and studying the supply chain attacks
	ENI (2022)	Identifying the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis
	Chowdhury et al. (2023)	Study application of ChatGPT to attack supply chain
Health Care Supply Chain	Arora & Gigras (2018)	Study impact of supply chain on functioning of hospitals
	Snowdon et al. (2021)	Study impact of supply chain on proactive and comprehensive responses to pandemic management
	Carmody et al. (2021)	Building resilient medical technology supply chains with a software bill of materials
	EL Azzaoui et al. (2022)	Proposing a blockchain-Based distributed information hiding framework
Food Supply Chain	Mor et al. (2015)	Reviewing technological implications of food supply chain practices
	Wang et al. (2021)	Proposing a framework based on the consortium and smart contracts
	Ferdousi et al. (2020)	Proposing a permissioned distributed ledger for the beef cattle supply chain
ICS Supply Chains	Hou et al. (2019)	Security Requirements
Energy Supply Chain	Duman et al. (2019)	Modeling supply chain attacks in IEC 61850 substations
	Aslam et al. (2021)	Studying factors influencing blockchain adoption in supply chain management practices
	Kim et al. (2020)	Categorization of cyber attack in nuclear power plants
	Baezner & Robin (2017)	Retrospectively analyze Stuxnet
Maritime Logistics	Scholliers et al. (2016)	Improving the security of containers in port related supply chains
	Polatidis et al. (2018)	Cyber-attack path discovery in a dynamic supply chain maritime risk management system
IT Supply Chain	Boyson (2014)	A survey on cyber supply chain risk management

This paper is organized as follows. In Section 2, we discuss different security threats that can put a supply chain at risk, such as counterfeiting and device tampering. The vulnerabilities of different sectors against cyber threats are described in Section 3. In Section 4, we review traditional approaches that have been used to protect supply chains against physical security threats. Then, we focus on innovative technologies proposed to secure supply chains against cyber and physical threats in recent years in Section 5. We dedicate Section 6 to presenting our key findings from this survey study, which can be used to design guidelines for the security of the supply chain. Finally, we conclude the survey in Section 7, reflecting the main points presented in this survey, and in Section 8, provide suggestions for future studies for researchers.

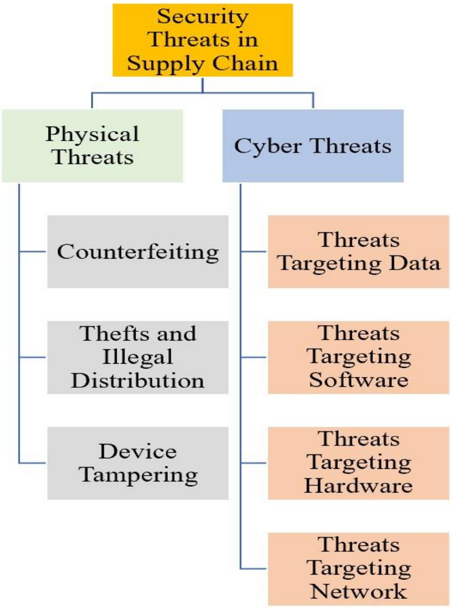

Security Threats in Supply Chain
Physical Threats
Cyber Threats
Counterfeiting
Thefts and Illegal Distribution
Device Tampering
Threats Targeting Data
Threats Targeting Software
Threats Targeting Hardware
Threats Targeting Network

Figure 2. A category of the threats in a supply chain

2. Security Threats in Supply Chain

Supply chain security is one of the major aspects of supply chain management processes that focus on security related to vendors, suppliers, logistics, and transportation Hassija et al. (2020). Security breaches can happen at various stages within the supply chain, including the sourcing of raw materials, the involvement of suppliers, production processes, distribution channels, and even within the marketplace itself Iro (2021). Therefore, the main objective of supply chain security is to identify, analyze, and mitigate the security threats that would affect the operations of the supply chain. Traditionally, supply chain security mainly focused on physical security related to products, but now cyber threats have become a critical concern as they target vulnerabilities in software and services related to the supply chain Hassija et al. (2020). Figure 2 shows a category of supply chain threats. In this section, we discuss security threats related to supply chains, specifically physical and cyber threats.

2.1. Physical Threats

As a supply chain involves raw materials and products that need to be stored and distributed, the physical security of logistics and transportation is a very crucial aspect of supply chain security. There are different security threats, such as counterfeiting, theft, and device tampering.

Counterfeiting: Counterfeiting and pirated products have become one of the major physical security threats globally as many industries have become victims of counterfeit products Coates (2019). According to a survey conducted by Forbes, counterfeiting has been identified as the most impacting criminal enterprise in 2018 Shepard (2018). These counterfeited products are generally low in quality and do not provide adequate functionalities. These substandard products affect the sales and profits of organizations not only causing a negative reputation, but also causing a risk to public health, safety, and security Verma et al. (2019).

Thefts and Illegal Distributions: The lack of physical security implementations on logistics and transportation leads to the physical threat of thefts, where perpetrators can steal products and bring them back into the legitimate supply chain Buckley & Gostin (2013). In many developing countries, inadequate storage facilities have become a major issue for industries like pharmaceutical and food suppliers. Unfortunately, due to poor quality and safety standards, these industries are becoming victims of theft. This can lead to serious health and safety implications for consumers when the products are stored improperly or distributed unsafely. Therefore, it is crucial for all parties involved to prioritize physical security measures to prevent theft and guarantee product safety.

Devices Tampering: Thanks to the Internet of Things (IoT) technology, IT has become more integrated into supply chains by employing IoT devices to monitor production, storage, and transportation. However, this increased involvement also introduces the risk of device tampering, wherein genuine hardware can be substituted with defective counterfeit or tampered hardware. Such actions have the potential to generate inaccurate data and disrupt the entire supply chain. Furthermore, tampered devices pose a threat to end customers, as they can execute unauthorized functions when utilizing the final product, potentially causing harm. One of the oldest device tampering attacks on the supply chain happened in 2015 when hackers planted malicious chips in motherboards manufactured by Super Micro Computer Inc. Sup (2018).

With the Internet of Things (IoT) technologies, supply chains are getting involved with more hardware devices, as these IoT devices are used for monitoring production, storage and transportation. One of the major issues with hardware devices is that they bring device tampering threats where legitimate hardware is replaced with faulty counterfeit or tampered hardware. Tampered hardware can produce unreliable information and affects the entire supply chain. It can harm the end customers by deploying unauthorized functions when the customers use the end product. One of the oldest device tampering attacks that targeted the supply chain happened in 2015 when hackers planted malicious chips in motherboards manufactured by Super Micro Computer Inc.

Table 2. Summary of Cyber Threats and Recent Examples

Cyber Threats	Examples
Targeting Data	Magacart Malware Mag (2019), Brenntag Ransomware Abrams (2021a), KIA Ransomware Abrams (2021b) Ransomware attack on Ukrainian energy companies Herr et al. (2020)
Targeting Software	Cloud Snooper attack Scroxton (2020), DoS attacks Nicholson (2022), Security Assertion Markup Language (SAML) attack Kaiser & Vincent (2019), NotPetya Banerjea (2018)
Targeting Network	SolarWinds attack ENI (2021b), Kaseya attack ENI (2021a), Crypto-mining worm Fishbein (2021); Doman (2020), Kubernetes attacks Robinson & Fishbein (2021), Ransomware attacks Cimpanu (2020a); Hashim (2021)

2.2. Cyber Threats

With the modern-day market requirements, suppliers, manufacturers, customers, and service providers span multiple geographical areas, where collaboration is required between them to manage the supply chain. Therefore, modern SCM is often achieved through different digital services, such as IT systems, networks and software. As the entire supply chain process involves critical information on materials, suppliers, productions and customers, organizations use digital storage to store and analyze this information. Also, organizations share this information with collaborators and other stakeholders through networks, mainly through internet-based approaches. Furthermore, organizations use different software developed by third-party organizations for the SCM process. Even though digitization has improved the efficiency and accuracy of this process, this digitization exposes the supply chain to several cyber threats, such as threats targeting the data, threats targeting the software and threats targeting the network ENI (2021b). Table 2 shows a summary of cyber threats and recent examples.

By compromising a single supplier, attackers can get access to its distribution systems and convert any application that is sold, any software update that is pushed, and any physical equipment that is shipped to customers into destructive Trojan horses. A single well-coordinated and organized attack can cause significant damage to many individuals and businesses involved in the supply chain. It is crucial to take precautions and ensure that proper security measures are in place to prevent such cyber-attacks from occurring.

2.2.1. Threats Targeting the Data

For any supply chain, securing its data is essential, as it ensures critical sensitive information related to materials, suppliers, productions and customers are stored and shared securely ENI (2021b). This information is stored using different digital devices and accessed and shared through networks. There are several cybersecurity threats that target information, especially breaching confidentiality, integrity, and availability Fernando et al. (2023). Table 2 includes a summary of cyber threats and recent examples that targeted data.

Confidentiality of Data: Confidentiality ensures that sensitive critical information is protected from unauthorized disclosure. Ensuring confidentiality is crucial in SCM, as this data might contain trade secrets Hassija et al. (2020). However, cyber threats such as malware and social engineering attacks can leak the data to the outside and breach the confidentiality of data ENI (2021b). The most frequent form of malware is spyware that gets installed in digital devices and collects data without the knowledge of the users. Phishing is one of the frequent forms of social engineering, where the user is convinced to disclose the information to unauthorized people. These attacks can happen through external and internal attackers, including employees, professional hackers and malicious competitors. According to the European Union Agency for Cybersecurity (ENISA) ENI (2021b), around 58% of supply chain cyberattacks are aimed at gaining access to customer data, including personal data and intellectual property. Magecart is a well-known malware in the supply chain industry that has compromised numerous e-commerce platforms and collected customers' credit card data Mag (2019).

Integrity of Data: Integrity ensures consistency, accuracy, and reliability of sensitive critical information. One of the key features of a supply chain is provenance which enables tracking the origin and flow of products throughout the supply chain Xiujuan Wang (2018). It makes the entire production procedure transparent and builds trust between the stakeholders. Therefore, the authenticity of the information related to the supply chain plays a significant role, and preserving the integrity of sensitive information is vital. However, cyber threats, such as Trojans, get downloaded onto digital devices disguised as legitimate programs, get installed and modify data without the knowledge of the users. Thus, inaccurate and wrong data may result in product delivery failures, profit losses, and trust issues between stakeholders.

Availability of Data: Availability ensures that the information is available to legitimate authorized stakeholders on time. A supply chain is built around different stakeholders. They require a variety of data at different points of the supply chain process. Cyber threats, such as ransomware and Denial-of-Service (DoS) attacks, breach the availability feature of information. Ransomware is generally a software program to encrypt files on a device, making any file and the system that rely on it unusable. Attackers who deploy the ransomware then demand ransom in exchange for decryption. In May 2021, Brenntag, a world-leading chemical distribution company, suffered from a ransomware attack. The attackers encrypted around 150GB of their data, and the organization had to pay 4.4 million dollars in Bitcoin as the ransom to retrieve the encrypted files Abrams (2021a). Kia Motors America (KMA), which has nearly 800 dealers in the USA, suffered a ransomware attack in February 2021, where the attackers demanded 20 million dollars in ransom for a decryptor and not to leak stolen data Abrams (2021b). A DoS attack targets information, machines, and devices and causes information and resources to become unavailable to intended users. One of the oldest DoS attacks that targeted the supply chain happened in December 2015, when hackers remotely compromised the information systems of three Ukrainian energy distribution companies and disrupted the electricity supply to the consumer Herr et al. (2020).

2.2.2. Threats Targeting Software

Modern organizations rely on various third-party software solutions for their supply chain management (SCM) processes, introducing potential risks that may be challenging to mitigate entirely Hammi & Zeadally (2023). Attackers compromise this third-party software using different types of attacks, such as malware, ransomware, and DoS, that could result in interruptions, destruction, and breaches of the data, network, and services of the organizations that are using this software. According to IBM (2022), 13% of data breaches occurred via exploiting third-party software vulnerabilities. By compromising a single supplier, attackers can infiltrate the distribution process and create thousands of victims, including different stakeholders in the supply chain. Moreover, the security of the IT devices used by retailers, distributors, and suppliers participating in the sale, delivery, and production of some software is crucial for supply chain security Sof (2020). According to the Cybersecurity and Infrastructure Security Agency of the USA, the companies involved in the software supply chain are major targets of attackers seeking to gain access to the victim's partners and customers Cimpanu (2020b).

The SolarWinds attack ENI (2021b), which happened in 2020, is one of the hard-hitting supply chain attacks in the last few years that exploited the software vulnerabilities of the supply chain. SolarWinds Orion is a network and application monitoring platform used by several organizations around the globe. The attackers compromised the infrastructure of Orion software and distributed malware known as Sunburst to Orion users. Around 18,000 organizations and government entities that were using Orion software were infected, and information such as user IDs, passwords, financial records, and source code was exposed to the attackers.

The Kaseya attack ENI (2021a), which happened in July 2021, is another major supply chain ransomware attack that exploited the software vulnerabilities of the supply chain. Kaseya VSA is a remote management and monitoring tool used by several organizations, especially service providers. A hacking organization called REvil launched a ransomware attack on Kaseya VSA, demanding payment of $70 million from Kaseya. Around 1500 companies that were using Kaseya VSA were affected ENI (2021b). The NotPetya ransomware attack, which was deployed in 2017, targeted the vulnerabilities of the Windows operating system and affected thousands of computers worldwide. It encrypted the hard drive of infected computers Banerjea (2018). Worldwide organizations such as Maersk (a shipping and logistics company) and Merck (a pharmaceutical company) were affected by the NotPeya attack. As a result, their supply chain process was disrupted. Table 2 includes a summary of cyber threats and recent examples that targeted software.

2.2.3. Threats Targeting Hardware

In the electronics industry, supply chains are commonly characterized by extensive networks that link global buyers with electronic hardware manufacturers and assemblers. However, the involvement of multiple intermediaries poses significant challenges in ensuring the integrity of components throughout the supply chain. Particularly, within the Integrated Circuits (ICs) production line, various vulnerabilities arise at different stages of the manufacturing process. These vulnerabilities encompass a range of threats, including counterfeit replicas, side-channel attacks, reverse engineering, Intellectual Property (IP) hijacking, and hardware Trojans. Table 3 provides a comprehensive overview of hardware-based attacks targeting different entities within the semiconductor manufacturing process Shamsoshoara et al. (2020). These attacks can be broadly categorized into two classes.

The first category of hardware-based attacks pertains to adversaries who lack physical access to the target device but exploit vulnerabilities in the device's software or network connections. These attacks encompass a range of techniques employed to gain unauthorized access and manipulate the device from a remote location. By identifying weaknesses in the software or network infrastructure, attackers can circumvent security mechanisms, extract sensitive information, or disrupt the normal functioning of the device. One prevalent example within this category is side-channel attacks, which capitalize on unintended information leakage, such as variations in power consumption, electromagnetic radiation, or timing patterns, to infer confidential data or cryptographic keys. By analyzing these side-channel signals, attackers can deduce critical information and compromise the device's security.

Table 3. Hardware-based attacks in the semiconductor manufacturing process

Manufacturing Process	**Hardware-based Attacks**				
	Hardware trojan	**IP hijacking**	**Reverse engineering**	**Fake replica**	**Side-channel**
Design (Architecture, logic, circuit, physical)	✓	✓	✓	✓	✗
Wafer Fabrication	✓	✓	✓	✓	✗
Verification and Test	✗	✗	✓	✓	✗
Packaging	✗	✗	✓	✓	✗
PCB Design	✗	✗	✓	✓	✗
User/Application	✗	✗	✓	✗	✓

The second category of hardware-based attacks, on the other hand, takes place when the attacker has direct physical access to the system or chip. At this level of closeness, the attacker has the chance to directly control or tamper with the hardware. For instance, they may engage in activities such as fabricating counterfeit replicas of the device or chip, reverse engineering the design to extract valuable proprietary information, or illicitly appropriating the Intellectual Property (IP) associated with the hardware.

It is crucial for the semiconductor manufacturing industry to address both classes of attacks and implement robust security measures at various stages of the production process. This includes implementing secure design practices, using tamper-evident packaging, conducting rigorous testing and validation, and establishing secure supply chain practices. By proactively addressing these vulnerabilities, the industry can enhance the overall security and trustworthiness of electronic hardware components, ensuring the reliability and integrity of devices used in critical applications.

2.2.4. Threats Targeting the Network

Supply chain has a distributed nature due to the large number of stakeholders which are geographically distributed. Computer networking plays a key role in automation, efficiency, and feasibility of some processes in a modern supply. For instance, nowadays, many customers can order online through e-commerce giants like Amazon from geographically widespread locations in the world. Despite all the benefits of networking, it exposes the supply chain to the network security threats such as snooping and DoS attacks.

An eavesdropping attack, which is known as a sniffing or snooping attack, can be considered as theft of data while being sent through the network. The cloud snooper attack, which was detected in 2020, used a rootkit to sneak malicious traffic through the victim organizations' Amazon Web Services (AWS) firewalls and installed a remote access Trojan (RAT) onto its cloud-based servers. It allowed the attackers to Command and Control (C2) servers and crafted requests to listen to inbound traffic to a targeted server for stealing sensitive data Scroxton (2020). As AWS is one of the largest cloud service providers and its services are used by several manufacturers and distributors worldwide, many organizations have faced the threat of Cloud Snooper attack Quist (2021). The Golden Security Assertion Markup Language (SAML) attack was an incident where attackers gained complete control of cloud systems and got access to SCM systems of around 18,000 organizations and government entities. This attack compromised SAML messages when SAML was used as the standard for exchanging authentication and authorization data between cloud users and applications Kaiser & Vincent (2019). Golden SAML was also used in the SolarWinds Orion attack ENI (2021b).

Cloud networks are becoming victims of DoS attacks more frequently, as the COVID-19 pandemic situation made a wide variety of systems to be digitized and managed through cloud networks. AWS was affected by a large-scale Distributed DoS (DDoS) attack in February 2020. It is considered to be the most extreme DDoS attack in recent history because it targeted an unidentified AWS customer using an approach named Connectionless Lightweight Directory Access Protocol (CLDAP) reflection. The attack amplified the data amount sent to the victim's machine by 56-70 times. The attack continued for three days, and at the peak, the network carried 2.3 terabytes per second, which made it impossible for legitimate users to access the network Nicholson (2022).

Cryptojacking, also known as cryptomining, is a type of cyber threat where an attacker uses a victim's computing power to generate cryptocurrency without the knowledge of the target. Cloud networks are becoming targets of crypto-jacking, as cloud infrastructure is rich with computing resources. As the cloud computing resources are being used by the attacker, legitimate cloud users might not be able to use the computing resources and encounter a DoS situation. In August 2020, the first crypto-mining worm was deployed on Linux servers in the cloud environment Fishbein (2021), followed by another crypto-mining attack in June 2021 to steal AWS credentials Doman (2020). Kubernetes (also known as K8s) is a popular platform for container orchestration in cloud architecture. It is also becoming a target of cybercriminals as they try to exploit vulnerabilities of Kubernetes applications, such as Argo Workflows Robinson & Fishbein (2021). Furthermore, cloud providers are becoming targets of ransomware attacks as attackers are demanding huge ransoms to decrypt the files with information stored in the cloud infrastructure. Cloud service providers such as BlackBaud Cimpanu (2020a) and Swiss Cloud Hashim (2021) were victims of recent ransomware attacks. Table 2 includes a summary of cyber threats and recent examples that targeted network.

2.3. Attacks Targeting the Suppliers and Customers

A supply chain attack can target any supply chain's stakeholders, such as a supplier or a customer and their assets ENI (2021b). Therefore, supply chain attacks can be categorized based on their targets, such as suppliers or customers, and their respective assets.

Attacks Targeting the Suppliers: Table 4 shows six main attack types faced by the supplier of a supply chain in 2021 ENI (2021b). We have included a few examples of attack types and attack purposes. It is noted that each threat may be exploited using different.

Table 4. Attacks faced by the suppliers

Attacks	Types	Purposes
Malware Infection	Virus, Worms, Trojan, Ransomware	Gain unauthorized access to system and information
Social Engineering	Phishing, Spear phishing, Whaling, Spam	Impersonation and convincing the victim carry out a task
Brute-Force Attack	Password Attacks	Guess login information and gain unauthorized access
Code Injection	SQL injection, Buffer overflow	Gain unauthorized access and execute unauthorized commands
Misconfiguration	Misconfigured devices/ operating systems	Gain unauthorized access and execute unauthorized commands
Physical Attack	Counterfeiting, Thefts, Tampering	Modify/destroy hardware

Attack types (one or more) and the attack purpose. According to ENISA ENI (2021b), where they have studied 24 major supply chain attacks that were reported from January 2020 to early July 2021, software vulnerabilities have exposed 16% of the suppliers to cyber threats. Also, in most of the reported cases, victims do not know the attack type attackers used or the purpose of the attack. The same report indicates that 66% of the suppliers are unaware of the vulnerability exploited by the attacker. Generally, there is a direct relationship between the ultimate objective of the attack and the targeted asset, and therefore, it is possible to understand the objective of the attacker by analyzing the affected assets. According to recent surveys, 66% of attacks targeted to compromise supplier’s code, 20% of attacks targeted to compromise supplier’s data and 12% of attacks targeted to compromise supplier’s processes ENI (2021b).

Attacks Targeting the Customers: Table 5 shows four main attack types faced by the customer of a supply chain ENI (2021b) in 2021 with example scenarios. As mentioned previously, one or more vulnerabilities can be used to conduct an attack, and customers may not be aware of the exploitation techniques used by attackers. Also, it is noted that a customer can be exposed to the attack through a vulnerability at the supplier end and vice versa. According to ENISA’s survey, 62% of the attacks were carried out by abusing the trust of the customer (drive by compromise) ENI (2021b).

According to recent surveys, 58% of attacks targeted to compromise customer’s data, 16% of attacks targeted to compromise customer’s people and 8% of attacks targeted to compromise customer’s financial resources ENI (2021b). These statistics highlight the importance of information security.

3. Supply Chain in Critical Application Domains

Depending on the technologies used in an industry, a supply chain can face different security challenges Alshurideha et al. (2023). For example, 3D-printing can be used for mass.

Table 5. Attacks faced by the customers

Attack Type	Examples
Drive-by Compromise	Malicious scripts/ links in a website to infect users with malware
Phishing	Messages impersonating the supplier, fake update notifications
Malware Infections	Remote Access Trojan (RAT), backdoor, ransomware
Physical Attack	Modifying hardware, physical intrusion, create fake devices, impersonation of supplier’s personnel

customization and production according to open-source designs in agriculture, healthcare, aerospace, and automotive industry Shahrubudin et al. (2019). As 3D printing is susceptible to security issues, the aforementioned industries should consider the risk of using this technology. In this section, we highlight specific security issues which make supply chains in different sectors vulnerable and discuss the solutions provided in the literature. Particularly, we refer to the technologies and methods which have been applied to enhance security in industries. These technologies and techniques are described in detail in the following subsections.

3.1. Health

The healthcare sector deals with privacy-sensitive data such as the personal information of patients and their medical histories. Supply chains in the healthcare sector refer to the provision and distribution of medicine and cleaning products between hospitals and clinics to meet the medical needs of patients in a timely manner and the movement of employees among healthcare sites Arora & Gigras (2018). Despite the privacy-sensitive data in the healthcare sector, the related supply chains are underdeveloped compared to other sectors, such as the private sector Snowdon et al. (2021). Public health as one of the sixteen critical infrastructure sectors, is significantly at risk of unauthorized access from intruders Carmody et al. (2021). In recent years, medical supply chains have not been under sufficient security measures and encountered cyber-attacks which put data privacy at risk EL Azzaoui et al.
(2022).

One of the security concerns in healthcare supply chains is counterfeiting. Gokhale Gokhale (2021) has explained how hospitals can be protected against counterfeiting in the supply chain. Additionally, as healthcare supply chains become smarter and more connected thanks to the Internet of Medical Things (IoMT), they face more security challenges. For example, hackers may use vulnerabilities in IoMT systems to attack medical devices. Asset-tracking systems in hospitals are another potential target for hackers Gokhale (2021). These systems are responsible for the availability and accessibility of all products, consumables, and IoMT devices. Most of these assets are managed by their suppliers on behalf of hospitals, and suppliers issue invoices when an item is used. Both hospitals and suppliers need that all transactions, including ordering and invoicing, are secure.

Vulnerabilities of third-party components can have a significant impact on healthcare delivery. In the era of IoMTs, even a single defect in the software program of a device can put the patient in a life-or-death situation. Thus, a critical concern in the health supply chain is the security of the third-party software used in IoMTs. In 2017, an attack exploiting a vulnerability in several versions of Microsoft Windows infected 200,000 computers across 150 countries Piper (2017). During the same year, the US Health and Human Services Cybersecurity Task Force declared the critical condition of healthcare cybersecurity due to software vulnerabilities. The risk exposed by the third-party software can be managed by a Software Bill of Materials (SBoM), which is similar to the list of ingredients on food products Carmody et al. (2021). SBoM is a list of all software components which are used in an IoMT device. It eases the identification and remediation of vulnerabilities in software components. SBoM has been recommended by the federal government of the US to manufacturers and developers in order to enhance cybersecurity in the health sector. Other technologies can be used for cybersecurity purposes in the critical healthcare sector. Azzaoui et al. EL Azzaoui et al. (2022) proposed a framework for preserving data privacy in communication networks of smart healthcare supply chains. This framework can be implemented using Hyper-ledger smart contracts and achieve some level of data privacy according to the results presented in EL Azzaoui et al. (2022).

3.2. Agriculture

Nowadays, several problems exist in the traditional agricultural food supply chain, such as the large number of participants, inconvenient communication due to the long supply chain cycles, and distrust between the central system and participants Mor et al. (2015). Thus, it is difficult to keep track of product safety and quality issues in traditional agricultural food supply chains. Wang et al. Wang et al. (2021) leveraged blockchain to improve traceability in the food supply chains. A framework was proposed to track the workflow using the consortium blockchain and smart contract. This framework disperses the information among entities to eliminate the need for central agencies. This framework stores the information about the environment and growth of crops in the Inter-Planetary File System, and stores file IPFS hashes in smart contracts. This approach reduces the size of the ledger. Shanwei Lvfengyuan Modern Agricultural Development Co., Ltd. has applied the framework proposed in Wang et al. (2021) and benefited from the provided disintermediation and traceability using Quick Response (QR) codes.

Traceability plays an important role in the rapid identification of infected animals, which is crucial to control an infectious outbreak. Unfortunately, the traceability of animals is challenging. For example, the US Cattle Industry does not provide appropriate traceability. Although the U.S. Department of Agriculture (USDA) requires veterinary inspections for inter-state movement, the intra-state data are kept private by the farm owners Ferdousi et al. (2020). Several projects have been established to enhance the traceability of animals considering the data security based on mutual trust assumption among participants. The authors in Ferdousi et al. (2020) have used blockchain and smart contract technologies to resolve traceability issues.

3.3. Industrial Control Systems (ICS)

Critical infrastructures such as water distribution systems and power supply networks can be managed using Industrial Control Systems (ICSs), which are a kind of cyber-physical systems. According to the Industrial Control System-Cyber Emergency Response Team (ICS-CERT) in the USA, the number of attacks on ICSs has been increasing continuously within the last two decades Hou et al. (2019). For instance, the Maroochy Water Services, Iran’s nuclear plants, the German Steel Mill, and the Ukrainian power grid were attacked in 2000, 2010, 2014, and 2015, respectively, using vulnerabilities in hardware or software components of computer systems, networks, and human resources. Various standards and methods have been developed by the National Institute of Standards and Technology (NIST) and the UK Centre for Protection of National Infrastructure (CPNI) to combat cyber-attacks in ICSs. Moreover, the PA Consulting Group for CPNI has provided a practice guide for process control and Supervisory Control and Data Acquisition (SCADA) security. Unfortunately, these sources do not consider how security risks are managed and assessed by member organizations of the ICS supply chain, which impacts the security requirements Hou et al. (2019). Digital Components, including the software used in ICSs, are provided by one or more manufacturers or by external service providers, which expose the ICSs to different cybersecurity risks. The owner of an ICS has not gained enough control over the ICS supplier system. Technical and physical issues have been mainly considered in the risk assessments of ICSs. However, it is important to consider social, organizational, and human aspects in managing cybersecurity risks. Cybersecurity risks in an organization can impact another organization or even the full ICS supply chain. Hou et al. Hou et al. (2019) proposed a risk assessment framework for the ICS supply chain where they had taken into account a socio-technical system, including human resources, organizations, and software, hardware, physical parts.

3.4. Energy

Supply chains in the energy sector are crucial, and a cyber-attack can have a high impact from financial, national security, and national reputation perspectives. It can cause a blackout in other industries, which could adversely affect customer satisfaction and the economy. Supervisory Control and Data Acquisition (SCADA) systems, which can be used for remote monitoring and controlling purposes in gas or oil pipelines and power transmission systems, become more vulnerable, as declared by the ICS-CERT. In this subsection, we explain the vulnerability of different parts of the energy sector to cyber-attacks and some measures to protect against them.

Smart Grid: IEC 61850 substations are exposed to the risk of supply chain attacks. Duman et al. Duman et al. (2019) took the first step to the thorough analysis of supply chain attacks on IEC 61850 substations, which can exploit the vulnerabilities injected to a device by a misbehaving vendor or conducted by an attacker who has infiltrated into the distribution channel of a non-malicious vendor. Supply chain attacks can be largescale, coordinated, and automatic in the context of IEC 61850 substations and cause major damages, such as leaking sensitive data like cryptography keys. The authors in Duman et al. (2019) modeled these attacks under various scenarios, and the proposed concrete models were used to study the impact of supply chain attacks quantitatively using simulation. According to these experiments, layered defense makes a system more resilient to supply chain attacks. Securing the system against this kind of attack is very important as it may have a much higher impact on the system security than expected, particularly automated attacks. Based on Duman et al. (2019), increasing the number of communication channels in only one device can adversely affect the resiliency of the whole network.

Oil: The oil industry, a critical part of the energy sector, needs to prevent and mitigate cyber-attacks. For instance, an unauthorized intrusion in the information layer of the oil supply chain can cause the failure of the electrical power supply in the ordering system, which stops oil delivery to energy plants. Pakistan is not an oil-producer country, while oil is an indicator of economic development. As Pakistan needs to import a huge amount of oil, it has a complex oil supply chain, which is improving by adding some features like online financial transactions, order tracking, and scheduling. This shift necessitates effective IT components to make the chain secure against cyber-attacks. In Aslam et al. (2021), an empirical study on the oil supply chains in Pakistan is presented, indicating that using blockchain technology enhances operational performance as well as cybersecurity.

Nuclear Power: Digital instrumentation and control devices have made nuclear plants vulnerable to cyber-attacks. SCADA and ICS systems in a nuclear power plant can be targeted by attackers Kim et al. (2020). In 2010, an attack based on Stuxnet, a malicious computer worm of volume 500 *KB*, hit the nuclear facilities in Iran. This attack was initiated by the USB drive of an employee and resulted in over fifteen Iranian facilities being attacked and infiltrated by the Stuxnet worm Holloway (2015). Stuxnet caused severe damage to almost 20% of Iran's nuclear centrifuges by targeting industrial programmable logic controllers Baezner & Robin (2017). This attack destroyed the uranium enrichment facility in Iran. Cyber-attacks on the nuclear power sector can have more severe outcomes than other industries, given that leakage of radioactive radiation or illegal transfer of nuclear materials may be possible under cyber-attacks. In Kim et al. (2020), a countermeasure has been proposed to protect nuclear power plants against cyber-attacks.

3.5. Logistics

Logistics and shipping companies, which are involved in the supply chains, are vulnerable to cyber-attacks. For instance, in 2017, AP Moller Maersk, a Danish shipping company, lost millions of dollars due to the NotPeyta attack Cheung et al. (2021). Moreover, in 2020, Toll Group, a logistic company in Australia, was hit by two different ransomwares Lennane (2020); Marle (2020). Maritime logistics plays an important role in the global supply chain as goods are carried mainly by sea. Svitzer, an Australian maritime transportation company, is one of the major logistics service providers in the Australian supply chain. In 2017, Svitzer was hit by a group of attackers, and a data breach compromised some email accounts. It resulted in sending sensitive financial information to email addresses belonging to attackers Cheung et al. (2021).

The integrity of cargo containers should be ensured in ports and other terminals, and transportation of containers needs to be monitored for supply chain security Scholliers et al. (2016). A range of technologies can be used to protect containers at ports and for transferring containers. In addition to mechanical security, the integrity of containers can be verified automatically using the electronic seals attached to the door of a container. Custody and logistics benefit from the electronic seals as they ensure that the container has not been tampered with or opened during a transportation phase. Another technology used to protect cargo containers is Container Security Device (CSD) which can detect breaches and inform control centers using cellular or satellite communication. Battery lifetime and security against jamming and spoofing are important characteristics that should be taken into account while choosing container security devices Scholliers et al. (2016). The authors Polatidis et al. (2018) suggested a novel approach for identifying cyberattack pathways that may be applied in risk management systems. Since physical security is the primary focus of current risk management systems, this is especially crucial. It is evident that additional research is needed in this field, and investigating risk and vulnerability assessment in IT-enabled maritime transportation is a potential research direction.

3.6. Information Technology (IT)

Although the IT industry has developed some products, such as firewalls and intrusion detection systems, which can be used for cybersecurity purposes in other industries, the IT industry is also vulnerable to cyber-attacks. The supply chain can be considered a major threat vector in the IT industry. In 2011, as reported by Mike Rogers, the Chairman of the U.S. House of Representatives Intelligence Committee, cyber-attacks on the IT supply chain had caused a one trillion dollar loss in total revenue and loss of 10,000 jobs per year Boyson (2014). In the following, we explain some root causes of cybersecurity attacks that are relevant to the supply chain.

3.6.1. Globalization and Outsourcing

Globalization and outsourcing have been common practices in the IT industry since the last decade. For instance, about 20% of the computer chips used in the US electronics industry in 2014 were manufactured locally in the US, while 80% outsourced. Globalization and outsourcing, which are normal in most IT sectors, can be root causes of cyber-attacks due to increased attack surface. Cyber Supply Chain Risk Management (CSCRM) is a discipline that helps the IT industry to address security challenges raised by fast globalization and outsourced diffusion of computer system components Boyson (2014). CSCRM combines cybersecurity, supply chain management, and enterprise risk management practices. The three representative cybersecurity practices which help the IT industry mitigate the risk of outsourcing and globalization are: 1) Organizing an IT security group, including a chief information security officer and technical agents of operating modules, to determine security policies, 2) Screening hardware components and software codes developed abroad, 3) Providing hardware and software components from certified trusted manufacturers Boyson (2014).

3.6.2. Backdoors

Backdoor refers to a way of gaining access to a computer system or network through a hidden or unauthorized entry point. Many cyber-attacks can be conducted using the software or hardware backdoors that are inserted into the devices during the supply chain process. For instance, a malicious foreign vendor could put some backdoor in a device before shipment and use this backdoor to leak information. Backdoors had a major role in cyber-attacks in recent years, particularly due to the outsourcing of software and hardware components. Moreover, the recent advanced technologies such as generative AI can be used to establish realistic communications with supply chain users, and help the attackers to distribute and set up malware in the supply chain users devices Chowdhury et al. (2023). For instance, the *SolarWinds* attack Constantin (2020), as one of the biggest attacks in the 21st century, was based on a software backdoor, which had remained undetected for a long time.

Network infrastructures which are used to transfer information can be vulnerable to cyber-attacks due to the backdoors inserted by the vendors. It is very challenging to verify the trustworthiness and functions of complex network components such as switches. One may suggest avoiding using devices that seem to be untrusted based on their vendor, the country in which they are manufactured, etc. However, as there are a few manufacturers around the globe for state-of-the-art network devices, excluding even one of them can cause a significant delay in the supply chain process. For example, the UK has planned to replace some untrusted foreign network products in mobile service providers in seven years Kelion (2020).

4. Traditional Approaches for Physical Security

In the traditional supply chain, supply chain management (SCM) has been carried out in a centralized manner, where both the product manufacturing facility (headquarters) and product storage facility (warehouse) is located in a single location. Having a centralized supply chain provided several advantages, such as low cost, easy management, centralized decision-making, and higher product availability.

Supply chain security is one of the major aspects of the SCM processes that focus on security related to vendors, suppliers, logistics and transportation Hassija et al. (2020). Even though recent supply chain security approaches focus more on cyber-related threats, traditionally, supply chain security has mainly been focused on physical security related to products Hassija et al. (2020). Physical security included: (1) securing the physical facilities related to supply chains, such as manufacturing plants and storage locations, and (2) securing the raw materials and products. In this section, we will discuss traditional approaches that have been used to secure supply chains.

4.1. Securing the Physical Facilities

A supply chain includes physical facilities such as a manufacturing plant (headquarters), physical storage location (warehouse) and transportation and distribution mechanisms Coates (2019). Having a secured manufacturing plant and a warehouse with adequate traditional security measures such as locked doors, CCTV cameras and physical security personnel are essential to ensure the supply chain's physical security. The lack of physical security implementations on logistics and transportation leads to the physical threat of thefts, where perpetrators can steal products and reintroduce inferior-quality products back into the legitimate supply chain Buckley & Gostin (2013). Therefore, location tracking systems such as Global Positioning Systems (GPS) have been used to track the locations of distribution vehicles and to ensure the security of the distribution system.

4.2. Securing the Raw Materials and Products

Counterfeit products and raw materials are major physical security threats to the supply chain, and the most impacting criminal enterprises in 2018 Shepard (2018) were involved in counterfeiting. Identifying the originality of a product and tracking it from the manufacturing process through shipping to the end customer ensures the authenticity of a product and supply chain security. Several techniques have been used to identify and trace products as well as raw materials to ensure a secured supply chain.

4.2.1. Universal Product Code (UPC) and Electronic Product Code (EPC)

The Universal Product Code (UPC)[1] is a standard that is used in retail stores and supermarkets to identify the manufacturer and the class of each product. For the first time in 1974, it was used to scan an item in a supermarket. UPC consists of a barcode and a unique 12 digits' number. Barcodes are a series of lines and black bars in a unique sequence and can be read by barcode scanners. The 12-digit numerical code is called a GTIN (Global Trade Identification Number), which identifies the company (manufacturer) and the product.

The Electronic Product Code (EPC) is a successor to the UPC, where the Electronic Product Code (EPC) is used to identify each unique item. Each physical object has a unique EPC Brock (2001). EPC is a 96-bit number that distinguishes two identical products and also provides information about a product's manufacturer. In EPC, the Header field identifies the length, type, structure, version and generation of EPC. The EPC Manager field identifies the company or manufacturer uniquely and is assigned by the nonprofit standards organization the GS1 EPCglobal[2]. The object class and the serial number of an item are assigned by the EPC owner (products' manufacturer), conforming to the standards set by the GS1. The EPC standard outlines various categories of objects that can be labeled with RFID tags. These categories include trade items (e.g., raw materials and products), logistical units, location identifiers, returnable or reusable assets, fixed assets, documents, service relations (e.g., loyalty or library cards), U.S. Department of Defense supply chain items, aerospace and defense parts and items, technical industry components and parts, and a general category for unspecified objects. Both the UPC and EPC can be stored in a tag and attached to the product to enable traceability throughout the supply chain cycle. In Mainetti et al. (2013), authors proposed an EPC-based traceability system for vegetable plantations in Italy. Authors of Hwang et al. (2015) used EPC to identify and share product information in the Korean ginseng industry.

4.2.2. Radio Frequency Identification (RFID) Tags

The use of an RFID tag to identify each product uniquely has been helping to solve the counterfeiting threat for years Toyoda et al. (2017). RFID is a technology that uses radio waves to relay identifying information from an electronic tag placed on an object to an electronic reader. Some devices have used in World War II that can be considered a predecessor of RFID, but the first true ancestor of modern RFID devices was patented in 1973, and the first patent using RFID abbreviation was granted in 1983. The traditional way of using RFID in the supply chain involves the following. First, assign a unique code to each product (i.e., UPC or EPC), write that code into an RFID tag, and then attach the RFID tag to the product. Each stakeholder in different stages of a supply chain can read these tags using an RFID reader and write their data on them.

RFID tags are used in different industries, generally to track inventory. In manufacturing, products can be tracked from the manufacturing process through shipping to the end customer using RFID tags. In the retail industry, RFID tags are often attached to items in store as an anti-theft method. RFID technology can be used for long distances, up to 100 meters and do not require a direct line of sight to the reader. However, RFID tags are vulnerable to cloned tags Staake et al. (2005), and they cannot be used to track the product once it reaches the retail stores or sells the product to second-hand shops. In Toyoda et al. (2017), they divided the supply chain into two parts: RFID-enabled and post-supply chain. They proposed a method leveraging Bitcoin's blockchain for anti-counterfeit to be used in the post-supply chain.

[1] https://www.gtin.info/upc

[2] https://www.gs1.org/epcglobal

4.2.3. Quick Response (QR) Code

The QR code, introduced by Denso Wave in 1994, is a two-dimensional matrix barcode that allows digital devices to read and store information through a grid of pixels QR2 (2022). Denso Wave made their QR code technique publicly available, enabling universal access to QR code generation and utilization without pursuing patent rights. Unlike traditional barcodes, QR codes can be scanned in two directions (top to bottom and right to left) and store various forms of data, including website URLs, phone numbers, and text up to 4,000 characters. Widely adopted in supply chains for tracking product information, QR codes are also used in retail for quick access to product details, pricing, and promotions, enhancing the shopping experience. Furthermore, the hospitality industry utilizes QR codes for contactless check-ins, menu browsing, and secure payment processing, particularly in response to the COVID-19 pandemic. The seamless integration of QR codes into mobile devices and their ease of scanning have led to their acceptance by businesses and consumers. With ongoing technological advancements, QR codes are expected to further evolve and find innovative applications across sectors, improving efficiency and connectivity.

4.2.4. Near Field Communication (NFC) Tags

The Near Field Communication (NFC) technology evolved from RFID. It is specially used for small distances. For the first time in 2002, Sony and Philips worked together to create a technical outline for NFC and applied for the six fundamental patents of NFC. NFC has become popular in contactless payment systems as they provide a quick and simple way for consumers to pay using mobile applications. NFC tags are frequently used in pharmaceutical supply chains where each drug is registered and authenticated by using a key value and an NFC tag attached to it. Similar to an RFID tag, the user or the patient can verify the authenticity and the origin of the drug by scanning the attached NFC tag using a mobile application Musamih et al. (2021). Same as RFID, NFC tags also come in different formats, such as simple labels or hard tags.

4.3. Limitations of Traditional Security Approaches

Even though a centralized supply chain has several advantages, such as low cost and easy management, it introduces several challenges, including the authenticity of products, traceability, and delivery delays in the supply chain Alkhader et al. (2021). Furthermore, as the modern markets have become more distributed, where the stakeholders of supply chains span across different parts of the world, SCM is also changed into a decentralized approach.

Providing security for a decentralized supply chain is insurmountable because of several physical and cyber threats in the supply chain. Traditional security approaches, such as RFIDs and NFCs, are not enough to handle the cybersecurity challenges introduced by decentralized supply chains. Therefore, it is essential to incorporate recent technological advances such as blockchain, artificial intelligence, machine learning, and the Internet of things (IoT) to improve security in the supply chain.

5. Innovative Technologies to Enhance Security

In previous sections, we discussed the security threats a supply chain industry faces when employing traditional approaches in supply chain operations. We also highlighted security issues and vulnerabilities in different sectors of the supply chain. In this section, we provide insight for securing the supply chain with disruptive technologies.

5.1. Blockchain

The supply chain process includes all of the capabilities and functionalities related to product design, development, distribution, selling, support, consumption, and recycling. In the market, every product undergoes a series of interactions involving multiple stakeholders who collaborate intricately to bring the final offering to fruition. The complex nature of the supply chain poses significant difficulties in monitoring each step of the process. Unfortunately, some people take advantage of these difficulties and use different illicit practises, such as forgery and piracy, to advance their own financial interests. In today’s globalized world, supply chains have expanded across multiple geographic boundaries and socioeconomic dimensions, each with its own unique requirements for checks and balances. Ensuring the smooth operation of the supply chain under these circumstances can be a daunting task. Blockchain provides an ideal platform Hassija et al. (2019) for business stakeholders to tackle the issues of traceability, interoperability, and transparency in serving the need of modern supply chains. It is a decentralized technology that maintains the integrity of data in the distributed ledger between the contractually bound partners.

Characteristics: Blockchain technology is characterized by its distributed nature, operating on a decentralized platform where all participants have access to the same immutable ledger records Sabry et al. (2019); Arooj et al. (2022). This architecture allows participants to join or exit the network freely, enhancing the system's resilience against attacks. The immutable timeline of events, such as transactions, that blockchain may provide, allowing for transparent tracking and auditing of previous operations, is a key aspect. Because consensus among network users is used for transaction verification and approval, the likelihood of fraud is greatly reduced. The ledger's data is securely stored by sequentially linking and cryptographically hashing each transaction Haddad et al. (2022). This ensures that the integrity of the ledger is maintained and prevents tampering or unauthorized modifications. Even in the event of a compromised node within the network, it becomes infeasible for that node to persuade other nodes that its version of the blockchain is the valid one. The distributed nature of the ledger, combined with its replication across multiple independent nodes, ensures enhanced system security and trustworthiness Ruan et al. (2022). In the rest of this subsection, we explain how blockchain can be applied to provenance tracking and logistics management, which are part of supply chain.

5.1.1. Provenance Tracking

Provenance tracking within the supply chain involves validating the complete ownership, custody, and origin history of a specific product instance, such as a lot, batch, or serial number. This meticulous tracking plays a vital role in establishing trust among the various stakeholders involved in the supply chain ecosystem. Traditionally, inventory management in centralized systems has relied on barcodes, unique electronic product codes (EPC), and radio frequency identification (RFID) technologies to track items Epiphaniou et al. (2020). However, these systems are built upon centralized certificate authorities and databases, which introduce inherent security vulnerabilities. The presence of single points of failure within these systems makes them highly susceptible to counterfeit products and insider fraud.

Blockchain technology facilitates dependable provenance tracking by establishing an enduring record of the product's journey from its production to its sale, capturing every transaction whenever the product transitions to a new owner Min (2019); Peepliwal et al. (2022). With traditional supply chain procedures, this technology helps to cut down on human error, expenses, and delays. In order to address the challenges of the complicated supply chain for the international food business, Walmart and IBM teamed up in 2016 Network (2020). By integrating blockchain into the new system, suppliers gain the ability to digitally monitor food products at various stages of the chain, ensuring crucial information such as processing details, batch numbers, storage temperatures, expiration dates, and other relevant data is preserved Treiblmaier & Garaus (2023); Cruz & Ignacio (2023).

Case studies focusing on the pork supply chain in China and the mango supply chain in the US have demonstrated the effectiveness of blockchain technology Park & Li (2021). For instance, during events like an E. Coli bacteria outbreak CDC (2020), the improved turnaround time provided by blockchain can make a significant difference by swiftly identifying and containing contamination incidents, preventing them from escalating into viral outbreaks. Beyond the implications for public health, the enhanced efficiency throughout the entire system can lead to reductions in food waste, the prevention of fraud, and simplified regulatory compliance.

5.1.2. Logistics Management

Logistics is integral to effective supply chain management (SCM), facilitating the coordination, monitoring, and efficient movement of goods across stages. However, the absence of a unified data-sharing platform poses challenges for seamless, timely, and cost-effective information exchange among supply chain stakeholders Pratap (2018). Blockchain distributed ledger technology (DLT) appears as a viable remedy to this problem Andoni et al. (2019). By leveraging blockchain DLT, visibility and transparency are significantly enhanced, granting all participants access to accurate and real-time information, promoting collaboration and better decision-making. Automation reduces paperwork delays and optimizes logistics costs, while the technology also aids in detecting counterfeiting and preventing fraud, bolstering trust and integrity within the supply chain.

TradeLens, a collaborative initiative by IBM and GTD Solution Inc., is a blockchainbased open platform designed for supply chain management. TradeLens has established a global ecosystem that encompasses various stakeholders such as shippers, freight forwarders, terminal operators, ocean carriers, government authorities, customs brokers, and financial institutions Tra (2020). The primary goal of TradeLens is to streamline and digitize crossborder supply chain operations. By harnessing the power of blockchain technology, TradeLens ensures secure information sharing and collaboration among participants, resulting in reduced delays and minimized trade documentation. The platform's innovative approach revolutionizes traditional supply chain processes, bringing efficiency, transparency, and enhanced traceability to global trade operations.

5.2. Smart Contract

The term *smart contract (SCo)* was initially coined by Nick Szabo in 1997 Szabo (1997). Szabo's argument emphasized that smart contracts combine technology and promises communicated via interfaces. These contracts aim to formalize and secure relationships over public networks, establishing a solid basis for their practical implementation. The definition of smart contracts has been subject to rigorous scrutiny by several scholars Sillaber & Waltl (2017); Savelyev (2017) who have undertaken systematic assessments to uncover their inherent characteristics. For instance, Sillaber et al. Sillaber & Waltl (2017) delve into critical factors encompassing the contractual arrangements between involved parties, the governance of pre-conditions necessary for contractual obligations, and the actual execution of the contract. Savelyev Savelyev (2017) adopts a more nuanced perspective, bringing to light notable features such as the exclusive electronic nature, software implementation, heightened certainty, conditional behavior, self-performance capability, and self-sufficiency. Furthermore, Bottoni et al. Bottoni et al. (2020) succinctly summarize the primary features of smart contracts as automation, determinism, distribution, immutability, transparency, and trust.

The goal of an SCo is to streamline trade transactions, facilitating interactions between both anonymous and identified parties while potentially eliminating the need for intermediaries. They serve various purposes, such as automating payment releases, maintaining ledger entries, and signaling the requirement for manual intervention within the supply chain. SCos frequently complement and leverage the capabilities of blockchain technology, offering versatile applications across different use cases Wright & De Filippi (2015); Garrod (2016); Kosba et al. (2016); Nofer et al. (2017). SCos deployed on a blockchain network can overcome the inefficiencies inherent in manual invoicing systems by automating and digitizing contractual agreements. Adopting an SCo increases transparency, thereby helping to mitigate the possibility of corruption and fraud Weingartner et al. (2021).

5.3. Artificial Intelligence

Numerous companies are currently integrating cognitive technologies to harness advanced analytics and enhance supply chain operations. This strategic move enables businesses to unlock their full potential, resulting in time savings and risk reduction. According to McKinsey Global Institute, AI has the potential to increase global economic activity by approximately $13 trillion in 2030. A significant 81% of respondents, according to a survey conducted by Deloitte Chmielewski et al. (2021), said they intended to use new types of datasets to improve their analytical capabilities. Particularly within the shipping industry, organizations are making significant investments in the Internet of Things (IoT) and harnessing the advantages of data collection to gain valuable insights, exercise greater control, and improve visibility into their intricate supply chains. In subsequent sections, we discuss how AI is revolutionizing SCM.

5.3.1. Demand Forecasting and Inventory Management

Demand Forecasting and Inventory Management are crucial components of SCM that facilitate efficient planning, monitoring of goods flow, optimization of inventory levels, risk assessment, and management of demand exceptions. Nevertheless, employing inefficient demand forecasting strategies can have severe repercussions for organizations. Inaccurate forecasts resulting from such strategies not only undermine operational efficiency but can also result in significant financial losses El Hathat et al. (2023). For instance, failure to meet consumer demands due to inadequate supply can waste valuable time and resources while also causing customer dissatisfaction. Conversely, excessive supply, beyond demand, depletes critical resources without generating additional profits. The application of machine learning algorithms provides substantial advantages over traditional demand forecasting techniques Mahraz et al. (2022). They enhance data processing speed, resulting in faster insights, enable more precise forecasts, automate updates based on recent data, uncover hidden patterns within the data, facilitate the development of a robust system, and enhance adaptability to changes. By leveraging machine learning, organizations can streamline their demand forecasting processes, leading to improved decision-making, efficient resource management, and heightened customer satisfaction. This section highlights *DemandAI+* by Logility Logility (2023) as a sophisticated solution for demand forecasting, enabling businesses to anticipate market trends, consumer preferences, and demand fluctuations with precision. By harnessing data analytics and machine learning, it empowers organizations to make informed decisions, optimize inventory management, and enhance supply chain efficiency.

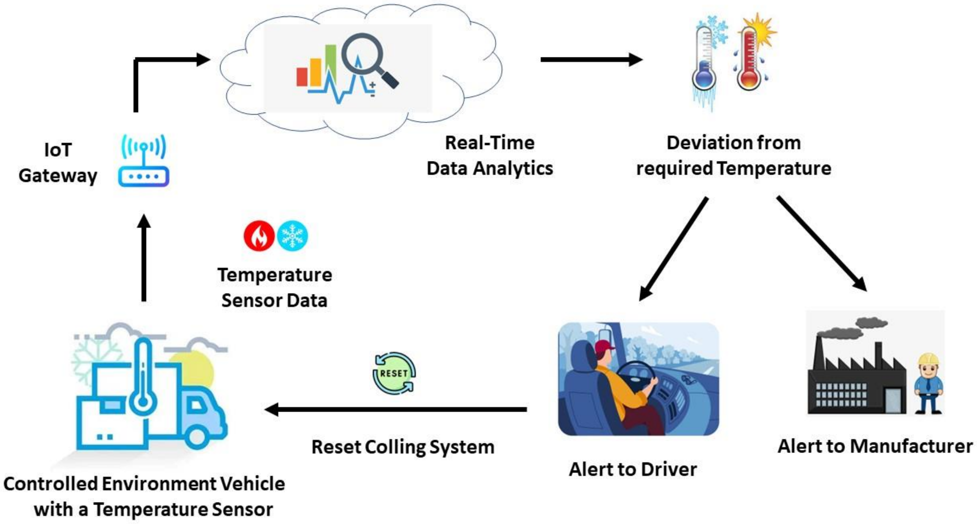


Figure 3. SCM using IoT connected tracking devices

5.3.2. AI-Powered Transit Monitoring

According to Zion Market Research ZMR (2022), the market for IoT sensors is witnessing significant growth and is expected to achieve a valuation of USD 27.9 billion by the year 2028. Prominent technologies such as GPS, GPRS, and RFID have emerged as indispensable tools in enabling real-time tracking of shipping vehicles, playing a vital role in monitoring the movement of goods and detecting critical concerns, particularly substantial delivery delays. The data derived from real-time vehicle tracking holds immense potential for optimizing predictive maintenance techniques. For instance, vehicles equipped with IoT sensors continuously monitor various parameters such as temperature, air pressure, and fuel levels, enabling AI models to promptly identify anomalies and provide real-time updates, as illustrated in Figure 3. This integration aids in identifying environmental hazards, enhancing operational efficiency, and reducing costs, thus contributing to improved performance within the supply chain.

5.3.3. AI-Powered Chatbots

Chatbots are recognized as conversational agents that engage with customers to address their inquiries. With the integration of artificial intelligence (AI) techniques such as natural language processing (NLP) and voice recognition, chatbots have revolutionized the interaction between logistics providers and customers by tailoring support to individual needs. IBM conducted a comprehensive assessment of 15 AI virtual assistant solutions and identified 'Watson Assistant' as the top-performing and most accurate option. According to the IBM report IBM (2018), AI-enhanced virtual agents can considerably lower labor costs by reducing the need for human intervention, potentially lowering customer support service costs by up to 30%. Additionally, they have the ability to handle approximately 80% of everyday duties and consumer inquiries. By leveraging AI-infused chatbots, supply chain operations can achieve a seamless flow of information, allowing them to effectively manage diverse data forms such as customer orders, real-time tracking, and fleet information.

As an innovative technology, applying AI chatbots comes with some challenges, such as the need for extensive training data to ensure accurate natural language processing, addressing potential ethical concerns, and ensuring the chatbot's responses align with company values and policies Adnan et al. (2021). Despite these challenges, AI chatbots have been widely applied in various sectors.

5.3.4. AI-Powered Self-Driving Vehicles

Self-driving or autonomous vehicles are equipped with an array of sensors, cameras, radar systems, and powered by Artificial Intelligence (AI), enabling them to autonomously navigate from origin to destination without human intervention Gupta et al. (2021). The utilization of these advanced technologies holds tremendous potential to bring about a transformative impact, primarily attributed to their ability to operate safely by continuously sensing the surrounding environment and making intelligent decisions based on real-time data. Autonomous vehicles have emerged as a substantial disruptive force within the commercial sector, with their influence further magnified by the repercussions of the pandemic. The shift towards online consumer shopping has brought about a significant surge in demand for trucking and last-mile delivery services, profoundly impacting supply chain operations. It is projected that this disruptive trend will continue and influence the industry's future, highlighting the continued significance of autonomous vehicles in satisfying the changing demands of the market.

Furthermore, the global shortage of drivers has escalated to alarming levels, posing a significant threat to the operational resilience of supply chains and an economy that is already grappling with the aftermath of a pandemic. The Driver Shortage Global Report 2022 by IRU IRU (2022) reveals that surveyed countries experienced an unfilled vacancy of over 2.6 million truck driver jobs in 2021, with projections indicating a further exacerbation of the shortage in 2022. Consequently, a substantial number of autonomous driving services are being developed to harness these emerging opportunities, which are indispensable for the future of transportation.

The incorporation of AI-powered autonomous vehicle technology holds immense promise for driving substantial transformations within the supply chain, leading to noteworthy benefits such as cost savings, decreased transportation time, enhanced road safety, and minimized carbon emissions. Moreover, diverse autonomous technologies are being integrated throughout the supply chain, including the deployment of autonomous cranes at shipping ports, the utilization of automated forklifts in various facilities, and the implementation of automated order-picking systems within warehouses. These progressive advancements collectively contribute to shaping the future of transportation and exert a profound influence on supply chain operations, ushering in a new era of efficiency and optimization.

A key challenge in autonomous driving is cybersecurity, as it can be life-threatening in the event of a cyberattack. The cybersecurity of autonomous cars has been extensively studied in recent years Kim et al. (2021), and the research in this area is still ongoing. Interestingly, autonomous cars are used in some cities, like San Francisco, which shows remarkable progress in this area. So far, this experience has been promising, and the number of autonomous vehicles in real life is expected to rise in the near future, given the efforts and huge investments of giant tech companies like Tesla, NVIDIA, etc.

5.3.5. Challenges of AI Adoption in Supply Chain Management

The increasing concern about AI-related data breaches is particularly evident in the landscape of SCM, where the regular handling of vast amounts of sensitive information heightens the risk. These breaches often stem from inadequately secured databases or networks, providing malicious actors with avenues to exploit vulnerabilities and gain unauthorized access to sensitive data. Additionally, phishing schemes targeting weaker links in the supply chain, such as smaller suppliers with less stringent security protocols, pose significant risks. Furthermore, poorly secured application programming interfaces (APIs) used in data collection and AI model processing can be exploited to extract data or introduce malicious code, exacerbating cybersecurity vulnerabilities Richey Jr. et al. (2023).

AI adoption in SCM brings with it a host of challenges and limitations that organizations must navigate to unlock its full potential. A primary concern revolves around the inherent biases present in AI algorithms Ashok et al. (2022), particularly evident in algorithmic recommendations for suppliers. These biases, often rooted in historical data, have the potential to perpetuate inequalities and undermine Supplier Diversity programs, raising legal and ethical implications for SCM organizations. Moreover, the training process for AI systems in SCM necessitates access to vast amounts of high-quality data, a resource that is often inaccessible or poorly managed by supply chain partners, especially small and medium-sized enterprises (SMEs). Inadequate data governance hinders scalability and exposes businesses to legal risks, which makes it difficult for AI systems to optimize supply chain processes.

Furthermore, the downstream application of AI in SCM, while offering the promise of enhanced customer experiences, introduces ethical dilemmas such as algorithmic bias and misinformation. As AI systems increasingly influence decision-making processes, organizations must navigate these challenges to uphold fairness and transparency in their operations Morgan et al. (2023). Additionally, AI adoption in SCM requires rigorous strategies to address data privacy, regulatory compliance, and workforce readiness Budhwar et al. (2023). Without robust policies and infrastructure to safeguard against security breaches and ensure regulatory compliance, organizations risk compromising sensitive information and facing legal repercussions. To effectively navigate these challenges, a proactive approach to policy formulation, structural adjustments, and stakeholder engagement is essential Dwivedi et al. (2023). By fostering collaboration between human expertise and automated intelligence, organizations can mitigate risks, maximize the benefits of AI adoption, and cultivate a resilient and sustainable SCM ecosystem.

5.4. Physically Unclonable Function (PUF) Technology

Counterfeiters surreptitiously inject substandard or tampered products into the supply chain for monetary incentives. These inferior or malfunctioning products not only generate consumer dissatisfaction but also inflict financial and reputational damage upon the original manufacturers. However, the advent of Physical Unclonable Function (PUF) technology has offered a robust solution to combat product counterfeiting in the contemporary supply chain. PUFs leverage the inherent variations introduced during device fabrication to extract a distinctive fingerprint unique to each device. By leveraging this innovative approach, PUFs provide a robust layer of embedded security, effectively combating counterfeiting attacks and ensuring the authenticity and integrity of products within the supply chain. In the rest of this subsection, we elaborate on two applications of PUF in supply chain.

5.4.1. Device Authentication using PUF

In the context of device authentication, the initial measurement of a device’s parameter is referred to as the “original response”. This measurement is obtained by applying a specific input stimulus or addressing a specific memory location known as the “challenge”, and both the original response and challenge are stored on the server. Subsequently, when the same parameter is measured again with the same external stimulus, it is called a “response”. The pairs consisting of challenges and responses are known as Challenge-Response Pairs (CRPs), and they are commonly compared to verify the authenticity of the device.

During the registration and authentication phases of a PUF, the disparity between the challenge and response in a CRP is known as the CRP error. Notably, the works presented in Koeberl et al. (2012); Yu et al. (2016) serve as examples of device or entity authentication schemes. Moreover, the research conducted in Suh & Devadas (2007) has demonstrated how PUFs can be employed to authenticate individual Integrated Circuits (ICs) without the need for costly cryptographic primitives. Additionally, a group of studies Cortese et al. (2010); Devadas et al. (2008); Hristea & T¸iplea (2019); Huang et al. (2017) have proposed integrating PUFs into the RFID ecosystem. By leveraging the inherent variations in the manufacturing process of ICs, PUFs offer a secure, robust, and cost-effective approach to authenticate silicon chips. This feature makes PUFs an attractive solution for ensuring the secure authentication of RFID ICs.

5.4.2. Traceability using Blockchain and PUF

PUF technology presents a promising avenue for the development of efficient traceability solutions when combined with blockchain. Several scholars Falcone et al. (2021); Islam & Kundu (2019) have put forth innovative frameworks to enhance product traceability within the supply chain using PUF-based devices as smart tags and blockchain as a distributed ledger to record all product-related transactions.

In Islam & Kundu (2019), Islam and Kundu addressed the need for a secure binding of an Integrated Circuit's (IC) identity to the record stored in a blockchain database, recognizing that a transaction record alone may be insufficient to verify an IC's origin. By leveraging PUF technology, they establish a robust link between the IC and its blockchain record, ensuring a trustworthy and tamper-proof traceability solution. Furthermore, Falcone et al. Falcone et al. (2021) propose a comprehensive framework designed to enable companies to track their suppliers throughout the production and distribution of products until they reach the end consumers. This framework involves a series of coordinated steps that incorporate various stakeholders, information, and resources. A pivotal aspect of this framework is the physical coupling of a smart tag to the product during the production phase, facilitating its unique identification and addressing key challenges related to safety, tracking, and counterfeiting that are prevalent in existing supply chain technologies. By combining PUF-based smart tags and blockchain technology, these frameworks offer promising solutions to enhance traceability within supply chains, improve product authenticity verification, and ensure the safety and integrity of products throughout their lifecycle.

5.5. Integrating Traditional Supply Chain Methods with Innovative Technologies

While innovative technologies are essentially important to enhance supply chain security, there are several challenges that may arise when implementing them in existing supply chains. The authors of Lin et al. (2019) discuss several challenges of using blockchain to build a traceability system, such as data explosion on the blockchain, trust transfer, and sensitive information disclosure. In addition, adoption of innovative technologies may require high capital expenditures, replacements of hardware and software components, and employees training Tian (2016). Therefore, instead of solely implementing and depending on innovative approaches, supply chain management experts have always been keen on integrating traditional supply chain security approaches with innovative technologies to enhance the security of supply chains. The main idea behind the integration is to utilize the strengths brought by the well-established existing approaches and explore innovative technologies to enhance supply chain security.

The authors of Lin et al. (2019) propose a novel food safety traceability system that is designed by combining traditional Electronic Product Code Information Services (EPCIS) with blockchain technology. A unique identification, an EPC code, is assigned to individual foods or batches, while the blockchain is used to store proof information and key traceability information. The proposed system has been implemented on the Ethereum platform via smart contracts. The authors show that the integration of EPC and blockchain provides better tamper-proofing capabilities while alleviating the data explosion problem on the blockchain.

The research work on Tian (2016) focused on building an agricultural product supply chain traceability system by combining RFID tags and blockchain technology, targeting the Chinese agri-food markets to enhance food safety and quality while reducing losses during the logistics process. The authors of Toyoda et al. (2017) argue that the genuineness of RFID tags cannot be guaranteed in the post-supply chain, as the tags can be easily cloned in the public space. Therefore, the authors propose a novel Product Ownership Management System (POMS) based on blockchain for RFID-attached products. With the new POMS, a customer can reject the purchase of counterfeits even with genuine RFID tag information if the seller does not possess their ownership. The authors have implemented an experimental system using Ethereum and evaluated its cost performance.

The research described in Alzahrani & Bulusu (2018) introduced a decentralized supply chain model that integrates existing NFC tags with blockchain technology. This system aims to track and trace products while detecting modifications, cloning, and tag reapplication attacks. Additionally, in Aniello et al. (2019), the authors proposed a secure supply chain management system. This system incorporates PUF technology, blockchain, and smart contracts to create a tracking system for physical parts of supply chains, with the objective of combating counterfeiting. These research endeavors collectively demonstrate that integrating traditional supply chain security approaches with innovative technologies significantly enhances the security of supply chains.

5.6. Case Study of Innovative Technologies

In Ferdousi et al. (2020), the authors proposed a framework based on blockchain and smart contracts for tracing the US supply chain of beet cattle. To begin, they proposed a model for the beef cattle operation in the US. Their model has six components: Ranch, Stocker, Feedlot, Packer, Distributor, and Retailer. Animals might stay in different farms based on age and weight. The packer slaughters and packs the animals, then sends them to the Distributor. Finally, the consumers will buy the products from the Retailer.

They designed a system on the Ethereum platform that includes four main smart contracts and ensures data immutability. The proposed system also supports animal traceability, user anonymity, and data aggregation. The four smart contracts are Profile Manager, Farm Manager, Transaction Manager, and Trace Manager. Their system can perform several tasks, including user profile and farm management, business transaction processing, animal tracing, and data aggregation. For instance, users and farmers are registered using the Profile Manager and Farm Manager components. In order to perform a transaction between two farm owners, one of them creates the transaction using Transaction Manager. Then, the other farm owner confirms the transaction, and finally, information about each farm is updated accordingly by the Farm Manager. In order to enable the traceability of animals, each of their movements is recorded by a component called Trace Manager. Using this component, the number of movements and the detailed information about each movement can be retrieved. With data aggregation, the scientific community or industry can access summary data, including the average weekly growth of specific breeds, vaccine effectiveness, and growth enhancements due to certain diets. This information provides insights into trends and performance metrics that can help in decision-making processes while safeguarding the privacy of businesses.

They also performed a detailed evaluation of their system concerning user privacy, data security, provenance, secure data aggregation, fairness, reliability, computational costs, and integrity. To summarize, the provided case study shows how an innovative technology such as blockchain can overcome several technical issues in a specific industry while preserving the business partners' data security, privacy, and ownership.

6. Discussion

In this section, we present our key findings obtained from this research, which can be used to design guidelines for the security of supply chains. We first discuss the main threats faced by different stakeholders who are involved in the supply chain. Then, we highlight major findings regarding the approaches that can be used for cyber and physical security in supply chains.

According to the European Union Agency for Cybersecurity (ENISA) (previously known as European Network and Information Security Agency), ENI (2021c), supply chain threats have increased during the years 2020 and 2021 (i.e., during the pandemic). According to the annual survey conducted by BlueVoyant Blu (2021), the average number of supply chain cyber threats saw a 37% increase from 2020 to 2021. A supply chain attack can target any supply chain stakeholders and their assets ENI (2022). Traditionally, supply chain security mainly focused on physical security related to products. However, cyber threats have become a major concern to the supply chain industry, as it targets vulnerabilities of software and services related to the supply chain Hassija et al. (2020).

In the following, we present some results obtained from statistical studies that can provide good insights in order to improve the design and quality of a system and meet the requirements. According to ENISA ENI (2021b), malware infections, social engineering, software vulnerabilities, configuration vulnerabilities and physical attacks were the main attacks faced by suppliers in 2021. Different vulnerabilities in the supply chain process and the IT components can be exploited by cyber attackers. For example, software vulnerabilities have been the root cause of the attacks faced by 16% of the suppliers ENI (2021b). However, unfortunately, most of the suppliers are unaware of the vulnerability that was exploited by the attacker. Different suppliers' assets can be targeted by attackers. As mentioned in ENI (2021b), most attacks in 2021 compromised the supplier's source code, while data and processes were the second and third most targeted assets, respectively. Specifically, source code, data, and processes were targeted by 66%, 20%, and 12% of the attacks in 2021 ENI (2021b). Generally, it is possible to understand the objective of an attacker by analyzing the affected assets. There is a possibility of a direct relationship between the ultimate objective of the attack and the targeted assets.

The cyber-attacks on the customer of a supply chain in the year 2021 were mainly conducted using malware infections and social engineering. 62% of the attacks were carried out by abusing customer trust as a middle man ENI (2021b). It is noted that customers can be exposed to the attack through a vulnerability in the supplier end and vice versa. Data was the hardest-hit asset of customers, with a rate of 58%. Interestingly, around 15% of the attacks on the supply chain have targeted the human resource of customers. For example, the safety of the employees can be compromised by supply chain attacks. A cyber-attack can also put the financial resources of customers at risk, as 8% of attacks in 2021 targeted to compromise customers' financial resources ENI (2021b). Thus, as customer service is a top priority in any industry, the security of supply chains needs to be of the utmost importance.

Supply chains are a combination of networks that span multiple continents and countries where multiple suppliers, manufacturers, competitors, and customers are involved. The successful delivery of commodities within the supply chain relies on the collaboration and intricate interactions among the various stakeholders involved. Each commodity undergoes a sequential process involving multiple stages and transitions between stakeholders, highlighting the complexity and interdependence within the supply chain. There are many access points in the supply chain networks where an attacker can be an insider (i.e., any of the stakeholders) or an outsider who can exploit the vulnerabilities in the software, systems, cloud networks, and edge devices for their ulterior motives. As described in Section 4, there are various traditional approaches to protect the supply chain against physical threats. Our observation indicates that RFID tags are the most common approach used in supply chains. However, emerging technologies, as discussed in Section 5, are vital to connecting the dots in the supply chains. These technologies not only improve the efficiency of the processes but also defend against different forms of attacks, such as counterfeiting, tampering, eavesdropping, and IP hijacking. In this survey, we reviewed state-of-the-art technologies, namely blockchain, artificial intelligence (AI), and physically unclonable functions (PUFs), in the context of the supply chain.

Blockchain has unique properties Puthal et al. (2018) that make it ideal for adoption by stakeholders in many sectors such as health, energy, food, and automotive to tackle the issues of traceability, interoperability, and transparency in serving the needs of modern supply chains Hassija et al. (2019). TradeLens Tra (2020), an open supply chain platform based on blockchain technology, enables secure information sharing, enhances transparency, reduces paperwork delays, and improves logistics management for participants in the supply chain. Furthermore, in addition to these advancements in transparency and security, blockchain technology also provides opportunity of smart contracts to automate execution of transactions, which plays a key role in protecting the rights of different stakeholders in supply chain.

AI- and ML-based approaches are driving a transformative shift in supply chain management, bringing forth intelligent automation capabilities. According to Deloitte Chmielewski et al. (2021), a significant 81% of respondents have expressed intentions to leverage new types of datasets to unlock advanced analytics. In comparison to traditional demand forecasting methods, ML-based approaches offer compelling advantages. They enable swift data processing, enhance forecast accuracy, unveil hidden patterns in data, establish a resilient system, and adapt with agility to dynamic changes in the environment. AI-powered models play a pivotal role in monitoring goods by leveraging data collected from IoT sensors, enabling the detection of anomalies, and providing timely updates for improved operational efficiency and cost reduction. The integration of AI-infused virtual agents, as highlighted by IBM, holds immense potential for cost savings through reduced human labor requirements and the ability to manage a significant proportion of routine tasks and customer inquiries IBM (2018). These AI chatbots are adept at handling various types of data, such as order tracking and fleet information, empowering organizations with efficient and effective customer service. Furthermore, AI is reshaping the automotive industry by improving safety standards. Autonomous vehicles, with their ability to navigate safely by perceiving the environment and making intelligent decisions, are poised to make a substantial impact on the industry landscape.

PUF technology provides a robust solution to identify counterfeit devices in the modern supply chain through unique device identification. By incorporating deliberate variations during the fabrication process, PUFs enable the extraction of a distinctive fingerprint for each device. The semiconductor manufacturing process exhibits various vulnerabilities that can be broadly categorized into two classes Shamsoshoara et al. (2020). Firstly, attackers without physical device access exploit software or network connections to gain remote entry, potentially compromising cryptographic keys and disrupting the authentication mechanism.

Secondly, attackers with physical device access can engage in activities such as producing counterfeit replicas, reverse engineering, or IP hijacking. In response to these challenges, researchers Cortese et al. (2010); Hristea & T¸iplea (2019); Huang et al. (2017) have proposed integrating PUFs into the RFID ecosystem as a secure, robust, and cost-effective approach to authenticate silicon chips. This integration enhances the overall security and reliability of supply chain operations, safeguarding against counterfeit and tampered devices.

Among the innovative technologies, blockchain especially targets the security of supply chains. It can be considered a promising security solution in the future. The trend to use blockchain can be observed easily in the papers published by the research community and the efforts made by high-tech companies. AI- and ML-based technologies are also vital to improve traditional measures for infrastructure security. For example, a next-generation firewall (NGFW) performs deep packet inspection and adds a layer of intelligence to protect devices and companies from a broader spectrum of intrusions. Similarly, next-generation antivirus (NGAV) leverages machine learning to detect potential unknown threats via behavioral analysis that traditional antivirus signature-based solutions would miss.

These innovative technologies not only tackle security challenges but can also improve efficiency in the supply chain. Depending upon the problem at hand, they can be commissioned standalone or can be combined with one or more technologies for developing potential solutions. For example, blockchains, in combination with AI-based techniques, can identify consumer energy patterns and add value to the future provision of energy products or services. Similarly, AI coupled with IoT technology drives advanced data analytics without human involvement. PUF technology, in tandem with blockchain, can help to develop efficient traceability solutions Falcone et al. (2021); Islam & Kundu (2019). As we know, no system is 100% secure and efficient. There are certain limitations associated with blockchain technology, particularly concerning consensus, transparency, and performance. Blockchains employ various methods of achieving consensus among participants, often relying on majority voting. However, this reliance on majority voting can be exploited by coordinated groups of attackers with ulterior motives, potentially compromising the integrity of the system. While transparency is beneficial for auditing and establishing trust, complete transparency may not always be desirable in scenarios where participants' activities need to remain confidential. Nevertheless, it is crucial to acknowledge that the inherent immutability of blockchain ensures resistance against unauthorized modifications, offering a robust layer of security to the system. However, this immutability also presents challenges in managing inaccurate records or making updates and deletions when necessary. As a result, the storage capacity required to accommodate every transaction increases, leading to the accumulation of unnecessary data and potential performance issues. Furthermore, PUFs play a critical role in IoT security, although concerns remain regarding their reliability, particularly in relation to changes in the physical environment.

7. Conclusion

In this survey, we undertake a rigorous analysis of recent literature to explore the dynamic landscape of supply chain management, with a specific emphasis on both physical and cyber security aspects. Our primary objective is to establish meaningful connections between the realms of supply and demand while proactively addressing the diverse challenges and sources of security threats that permeate the supply chain ecosystem.

Throughout our investigation, we have successfully identified certain limitations inherent in traditional approaches to supply chain security. These conventional methodologies predominantly concentrate on fortifying physical security measures, encompassing aspects such as product and facility protection and often relying on established technologies such as EPC, QR codes, and RFID. However, our research takes a bold leap forward by delving into the exploration of cutting-edge technologies that hold immense potential for elevating operational efficiency and mitigating security concerns within the modern supply chain paradigm. Notably, our investigation encompasses the transformative realms of blockchain, artificial intelligence, and physically unclonable functions. These emerging technologies, when integrated with existing solutions, present a compelling opportunity to tackle the critical issues encountered in supply chain management.

By shedding light on the potential of these innovative technologies, our study seeks to reshape the landscape of supply chain security, thereby empowering organizations to cultivate more effective and efficient operations.

8. Future Studies

As researchers anticipate future studies in supply chain management, an intriguing direction unfolds through an exploration into the implementation of a blockchain-based framework to transform processes and foster trust among stakeholders. Utilizing blockchain's unique attributes, particularly decentralization and traceability, this initiative seeks to address key challenges related to traceability, interoperability, and transparency within supply chains. Simultaneously, upcoming research endeavors could involve a qualitative risk assessment to evaluate the adoption of blockchain. This exploration holds the potential to provide crucial insights into the risks and benefits associated with integrating blockchain technology into supply chain management.

In the realm of supply chain management, future studies could delve into the integration of advanced machine learning algorithms, specifically exploring deep learning models to enhance demand forecasting precision and responsiveness. This investigation aims to assess the efficacy of these algorithms in handling diverse and dynamic data sources, contributing to more accurate and adaptable supply chain planning. The societal impact of such advancements is poised to significantly reduce financial losses associated with inventory mismanagement, optimize production activities, and bolster overall resilience to market fluctuations.

Additionally, researchers may focus on innovative AI techniques to fortify the cybersecurity measures within autonomous vehicle systems used in supply chain transportation. This future study could investigate potential vulnerabilities in autonomous vehicle systems and develop robust security protocols to safeguard against specific cyber threats prevalent in the supply chain context. The societal impact of securing autonomous vehicles through advanced AI techniques includes enhanced safety on roads, reduced cybersecurity risks in supply chain logistics, and a positive environmental impact due to optimized transportation efficiency.

Furthermore, future studies could explore the application of machine learning models for predicting zero-day attacks in supply chain cyber threats. By integrating real-time event analysis and historical data, these studies aim to enhance predictive capabilities, providing supply chains with proactive cybersecurity measures against emerging threats. The societal impact of such predictive cybersecurity measures encompasses not only the resilience of supply chains to cyber threats but also the safeguarding of critical infrastructure systems, ensuring uninterrupted business continuity.

Acknowledgments

This study received financial support from the National Science and Engineering Council of Canada (NSERC) and the Canadian Institute for Cybersecurity (CIC).

References

Abrams, L. (2021a). Chemical distributor pays $4.4 million to DarkSide ransomware. https://www.bleepingcomputer.com/news/security/chemical-distributor-pays44-million-to-darkside-ransomware/.

Abrams, L. (2021b). Kia Motors America suffers ransomware attack, $20 million ransom. https://www.bleepingcomputer.com/news/security/kia-motors-americasuffers-ransomware-attack-20-million-ransom/.

Adnan, S. M., Hamdan, A., & Alareeni, B. (2021). Artificial intelligence for public sector: Chatbots as a customer service representative. In *The Importance of New Technologies and Entrepreneurship in Business Development: In The Context of Economic Diversity in Developing Countries* (pp. 164–73). Springer International Publishing.

Alkhader, W., Salah, K., Sleptchenko, A., Jayaraman, R., Yaqoob, I., & Omar, M. (2021). Blockchain-based decentralized digital manufacturing and supply for COVID-19 medical devices and supplies. *IEEE Access*, *9*, 137923–4.

Alshurideha, M. T., Alquqac, E. K., Alzoubid, H. M., AlKurdie, B., & AlHamad, A. (2023). The impact of cyber resilience and robustness on supply chain performance: Evidence from the uae chemical industry. *Uncertain Supply Chain Management*, *11*.

Alzahrani, N., & Bulusu, N. (2018). Block-supply chain: A new anti-counterfeiting supply chain using NFC and Blockchain. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143–74.

Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M., & Wilczynski, A. (2019). Towards a supply chain management system for counterfeit mitigation using Blockchain and PUF.

Arooj, A., Farooq, M. S., & Umer, T. (2022). Unfolding the blockchain era: Timeline, evolution, types and real-world applications. *Journal of Network and Computer Applications*, (p. 103511).

Arora, M., & Gigras, Y. (2018). Importance of supply chain management in healthcare of third world countries. *International Journal of Supply and Operations Management*, *5*.

Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., & Ghafoor, K. Z. (2021). Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, (pp. 1–27).

Ashok, M., Madan, R., Joha, A., & Sivarajah, U. (2022). Ethical framework for artificial intelligence and digital technologies. *International Journal of Information Management*, *62*, 102433.

Aslam, J., Saleem, A., Khan, N. T., & Kim, Y. B. (2021). Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *Journal of Innovation & Knowledge*, *6*, 124–34.

Baezner, M., & Robin, P. (2017). *Stuxnet*. Technical Report ETH Zurich.

Banerjea, A. (2018). NotPetya: How a Russian malware created the world's worst cyberattack ever. https://www.business-standard.com/article/technology/notpetyahow-a-russian-malware-created-the-world-s-worst-cyberattack-ever118082700261_1.html.

Booz-Allen, & Hamilton (2004). Engineering principles for information technology security (a baseline for achieving security), revision a. *NIST Special Publication*.

Bottoni, P., Gessa, N., Massa, G., Pareschi, R., Selim, H., & Arcuri, E. (2020). Intelligent smart contracts for innovative supply chain management. *Frontiers in Blockchain*, *3*.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*, 342–53.

Brock, D. L. (2001). The electronic product code (EPC)-a naming scheme for physical objects. *White paper*, .

Buckley, G. J., & Gostin, L. O. (2013). Countering the problem of falsified and substandard drugs. *Consensus Study Report - Institute of Medicine*.

Budhwar, P., Chowdhury, S., Wood, G., Aguinis, H., Bamber, G. J., Beltran, J. R., Boselie, P., Lee Cooke, F., Decker, S., DeNisi, A., Dey, P. K., Guest, D., Knoblich, A. J., Malik, A., Paauwe, J., Papagiannidis, S., Patel, C., Pereira, V., Ren, S., Rogelberg, S., Saunders, M. N. K., Tung, R. L., & Varma, A. (2023). Human resource management in the age of generative artificial intelligence: Perspectives and research directions on ChatGPT. *Human Resource Management Journal*, *33*, 606–59.

Carmody, S., Coravos, A., Fahs, G., Hatch, A., Medina, J., Woods, B., & Corman, J. (2021). Building resilient medical technology supply chains with a software bill of materials. *NPJ Digital Medicine*, *4*, 1–6.

Cheung, K.-F., Bell, M. G., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217.

Chmielewski, J., Daher, M., & Ghazal, O. (2021). Enabling holistic decisionmaking to create a more intelligent network - The future of movement of goods. https://www2.deloitte.com/us/en/insights/focus/transportation/intelligentsupply-chain-movement-of-goods.html.

Chowdhury, M., Rifat, N., Latif, S., Ahsan, M., Rahman, M. S., & Gomes, R. (2023). ChatGPT: The curious case of attack vectors' supply chain management improvement. *IEEE International Conference on Electro Information Technology*,.

Christopher, M. L. (1992). Supply chain. *Logistics and Supply Chain Management*.

Cimpanu, C. (2020a). Cloud provider stopped ransomware attack but had to pay ransom demand anyway. https://www.zdnet.com/article/cloud-provider-stoppedransomware-attack-but-had-to-pay-ransom-demand-anyway/.

Cimpanu, C. (2020b). FBI warns about ongoing attacks against software supply chain companies. https://www.zdnet.com/article/fbi-warns-about-ongoing-attacksagainst-software-supply-chain-companies/.

Coates, R. (2019). Counterfeits are still a major problem. https://www.scmr.com/article/ counterfeits_are_still_a_major_problem.

Constantin, L. (2020). SolarWinds attack explained: And why it was so hard to detect. https://www.csoonline.com/article/3601508/solarwinds-supply-chainattack-explained-why-organizations-were-not-prepared.html.

Cooper, M. C., & Ellram, L. M. (1993). Characteristics of supply chain management and the implication for purchasing and logistics strategy. *The International Journal of Logistics Management*, *4*, 13–24.

Cortese, P. F., Gemmiti, F., Palazzi, B., Pizzonia, M., & Rimondini, M. (2010). Efficient and practical authentication of PUF-based RFID tags in supply chains. In *IEEE International Conference on RFID-Technology and Applications* (pp. 182–8).

Cruz, L., & Ignacio, P. S. D. A. (2023). Application of blockchain disruptive technology in agri-food chains for sustainable development, a systematic review. *International Journal of Supply and Operations Management*, *10*.

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., & Khandelwal, V. (2008). Design and implementation of PUF-based ”unclonable” RFID ICs for anti-counterfeiting and security applications. In *IEEE International Conference on RFID* (pp. 58–64).

Doman, C. (2020). Team TNT – the first cryptomining worm to steal AWS credentials. https://www.cadosecurity.com/team-tnt-the-first-crypto-mining-wormto-steal-aws-credentials/.

Duman, O., Ghafouri, M., Kassouf, M., Atallah, R., Wang, L., & Debbabi, M. (2019). Modeling supply chain attacks in IEC 61850 substations. In *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)* (pp. 1–6). IEEE.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., AlBusaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., Carter, L., Chowdhury, S., Crick, T., Cunningham, S. W., Davies, G. H., Davison, R. M., D´e, R., Dennehy, D., Duan, Y., Dubey, R., Dwivedi, R., Edwards, J. S., Flavia´n, C., Gauld, R., Grover, V., Hu, M.-C., Janssen, M., Jones, P., Junglas, I., Khorana, S., Kraus, S., Larsen, K. R., Latreille, P., Laumer, S., Malik, F. T., Mardani, A., Mariani, M., Mithas, S., Mogaji, E., Nord, J. H., O'Connor, S., Okumus, F., Pagani, M., Pandey, N., Papagiannidis, S., Pappas, I. O., Pathak, N., Pries-Heje, J., Raman, R., Rana, N. P., Rehm, S.-V., Ribeiro-Navarrete, S., Richter, A., Rowe, F., Sarker, S., Stahl, B. C., Tiwari, M. K., van der Aalst, W., Venkatesh, V., Viglia, G., Wade, M., Walton, P., Wirtz, J., & Wright, R. (2023). Opinion paper: “so what if chatgpt wrote it?” multidisciplinary perspectives on opportunities, challenges and implications of generative conversational for research, practice and policy. *International Journal of Information Management*, *71*, 102642.

EL Azzaoui, A., Chen, H., Kim, S. H., Pan, Y., & Park, J. H. (2022). Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems. *Sensors*, *22*, 1371.

El Hathat, Z., Zouadi, T., Sreedharan, V. R., & Sunder M., V. (2023). Strategizing a logistics framework for organizational transformation: A technological perspective. *IEEE Transactions on Engineering Management*, 1–22.

Epiphaniou, G., Pillai, P., Bottarelli, M., Al-Khateeb, H., Hammoudesh, M., & Maple, C. (2020). Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security. *IEEE Transactions on Engineering Management*, *67*, 1059–73.

Falcone, A., Felicetti, C., Garro, A., Rullo, A., & Sacca`, D. (2021). PUF-based smart tags for supply chain management. In *The 16th International Conference on Availability, Reliability and Security*. Association for Computing Machinery.

Ferdousi, T., Gruenbacher, D., & Scoglio, C. M. (2020). A permissioned distributed ledger for the US beef cattle supply chain. *IEEE Access*, *8*, 154833–4.

Fernando, Y., Tseng, M.-L., Wahyuni-Td, I. S., Jabbour, A. B. L. d. S., Jabbour, C. J. C., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in malaysia. *Journal of Industrial and Production Engineering*, *40*.

Fiorini, P. d. C., & Jabbour, C. J. C. (2017). Information systems and sustainable supply chain management towards a more sustainable society: Where we are and where we are going. *International Journal of Information Management*, *37*, 241–9.

Fishbein, N. (2021). Rocke group actively targeting the cloud: Wants your SSH keys. https://www.intezer.com/blog/cloud-security/rocke-group-activelytargeting-the-cloud-wants-your-ssh-keys/.

Garrod, J. (2016). The real world of the decentralized autonomous society. *tripleC*, *14*.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*.

Gokhale, V. (2021). Protecting hospitals from supply-chain counterfeits and other security threats. https://www.securitymagazine.com/blogs/14-security-blog/post/96068protecting-hospitals-from-supply-chain-counterfeits-and-other-securitythreats.

Green, W. (2022). Cyber attack on supplier halts Toyota production. https: //www.cips.org/supply-management/news/2022/march/cyber-attack-onsupplier-halts-toyota-production/.

Gupta, A., Anpalagan, A., Guan, L., & Khwaja, A. S. (2021). Deep learning for object detection and scene perception in self-driving cars: Survey, challenges, and open issues. *Array*, *10*, 100057.

Haddad, A., Habaebi, M. H., Islam, M. R., Hasbullah, N. F., & Zabidi, S. A. (2022). Systematic review on ai-blockchain based e-healthcare records management systems. *IEEE Access*, *10*, 94583–615.

Hammi, B., & Zeadally, S. (2023). Software supply-chain security: Issues and countermeasures. *IEEE Computer*, *56*.

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*.

Hashim, A. (2021). Swiss cloud hosting provider suffered ransomware attack. https://latesthackingnews.com/2021/05/06/swiss-cloud-hosting-providersuffered-ransomware-attack/.

Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, *8*, 6222–46.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721–43.

Herr, T., Lee, J., Loomis, W., & Scott, S. (2020). Deep impact: States and software supply chain attacks. https://www.atlanticcouncil.org/commentary/feature/deepimpact-states-and-software-supply-chain-attacks/.

Holloway, M. (2015). Stuxnet worm attack on Iranian nuclear facilities. http://large. stanford.edu/courses/2015/ph241/holloway1/.

Hou, Y., Such, J., & Rashid, A. (2019). Understanding security requirements for industrial control system supply chains. In *IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)* (pp. 50–3). IEEE.

Hristea, C., & T¸iplea, F. L. (2019). A PUF-based destructive private mutual authentication RFID protocol. In *Innovative Security Solutions for Information Technology and Communications* (pp. 331–43). Springer International Publishing.

Huang, H.-H., Yeh, L.-Y., & Tsaur, W.-J. (2017). PUF-based protocols about mutual authentication and ownership transfer for RFID Gen2 v2 systems. In *Transactions on Engineering Technologies* (pp. 49–59). Springer.

Hwang, Y., Moon, J., & Yoo, S. (2015). Developing a RFID-based food traceability system in Korea Ginseng industry: Focused on the business process reengineering. *International Journal of Control and Automation*, *8*, 397–406.

Islam, M. N., & Kundu, S. (2019). Enabling IC traceability via blockchain pegged to embedded PUF. *ACM Transactions on Design Automation of Electronic Systems*, *24*.

Kaiser, D., & Vincent, S. (2019). Analysis and detection of golden SAML attacks. *Report*, .

Kelion, L. (2020). Huawei 5G kit must be removed from UK by 2027. https://www.bbc. com/news/technology-53403793.

Khursheed, A., Kumar, M., & Sharma, M. (2016). Security against cyber-attacks in food industry. *International Journal of Control Theory and Applications*, *9*, 8623–8.
Kim, K., Kim, J. S., Jeong, S., Park, J.-H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, *103*, 102150.

Kim, S., Heo, G., Zio, E., Shin, J., & Song, J.-g. (2020). Cyber attack taxonomy for digital environment in nuclear power plants. *Nuclear Engineering and Technology*, *52*, 995–1001.

Koeberl, P., Li, J., Maes, R., Rajan, A., Vishik, C., Wo´jcik, M., & Wu, W. (2012). A practical device authentication scheme using SRAM PUFs. *Journal of Cryptographic Engineering*, *2*, 255–69.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *IEEE Symposium on Security and Privacy (SP)* (pp. 839–58).

La Londe, B. J., & Masters, J. M. (1994). Emerging logistics strategies: Blueprints for the next century. *International Journal of Physical Distribution and Logistics Management*, *24*, 35–47.

Lennane, A. (2020). Toll group resists ransom demands from hackers after cyber attack. https://theloadstar.com/toll-group-resists-ransom-demands-fromhackers-after-cyber-attack/.

Lin, Q., Wang, H., Pei, X., & Wang, J. (2019). Food safety traceability system based on Blockchain and EPCIS. *IEEE Access*, *7*.

Logility (2023). Ai-first demand planning how human-machine collaboration cuts costs, error, and implementation time.

Mahraz, M.-I., Benabbou, L., & Berrado, A. (2022). Machine learning in supply chain management: A systematic literature review. *International Journal of Supply and Operations Management*, *9*.

Mainetti, L., Patrono, L., Stefanizzi, M. L., & Vergallo, R. (2013). An innovative and lowcost gapless traceability system of fresh vegetable products using RF technologies and EPC global standard. *Computers and electronics in agriculture*, *98*, 146–57.

Marle, G. v. (2020). Toll refuses to pay cyber ransom as it acts to get its systems back online. https://theloadstar.com/toll-refuses-to-pay-cyber-ransom-as-it-actsto-get-its-systems-back-online/.

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business Logistics*, *22*, 1–25.

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *International Journal of Information Management*, *62*, 35–45.

Monczka, R., Trent, R., & Handfield, R. (1998). *Purchasing and Supply Chain Management* volume 8. South-Western College Publishing.

Mor, R., Singh, S., Bhardwaj, A., & Singh, L. (2015). Technological implications of supply chain practices in agri-food sector: A review. *International Journal of Supply and Operations Management*, *2*.

Morgan, T. R., Gabler, C. B., & Manhart, P. S. (2023). Supply chain transparency: theoretical perspectives for future research. *The International Journal of Logistics Management*, *34*, 1422–45.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., & Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access*, *9*, 9728–43.

Network, T. L. (2020). How Walmart used blockchain to increase supply chain transparency. https://theleadershipnetwork.com/article/how-walmartused-blockchain-to-increase-supply-chain-transparency.

Nicholson, P. (2022). Five most famous DDoS attacks and then some. https://www. a10networks.com/blog/5-most-famous-ddos-attacks/.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business and Information Systems Engineering*, *59*, 183–187.

Park, A., & Li, H. (2021). The effect of blockchain technology on supply chain sustainability performances. *Sustainability*, *13*.

Peepliwal, A. K., Narula, S., Sharma, R., Bonde, C., & Jain, K. (2022). Theoretical blockchain architecture model (t-bam) to control covid-19 related counterfeit medical products across supply chain. *International Journal of Supply and Operations Management*, *9*.

Piper, E. (2017). Cyber attack hits 200,000 in at least 150 countries: Europol. *Reuters*.

Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, *56*, 74–82.

Pratap, M. (2018). How is blockchain disrupting the supply chain industry? https://medium.com/hackernoon/how-is-blockchain-disrupting-thesupply-chain-industry-f3a1c599daef.

Puthal, D., Malik, N., Mohanty, S., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework. *IEEE Consumer Electronics Magazine*, *7*, 18–21.

Quist, N. (2021). TeamTNT actively enumerating cloud environments to infiltrate organisations. https://unit42.paloaltonetworks.com/teamtnt-operations-cloudenvironments/.

Ranathunga, D., Roughan, M., Nguyen, H., Kernick, P., & Falkner, N. (2016). Case studies of scada firewall configurations and the implications for best practices. *IEEE Transactions on Network and Service Management*, *13*, 871–84.

Richey Jr., R. G., Chowdhury, S., Davis-Sramek, B., Giannakis, M., & Dwivedi, Y. K. (2023). Artificial intelligence in logistics and supply chain management: A primer and roadmap for research. *Journal of Business Logistics*, *44*, 532–49.

Robinson, R., & Fishbein, N. (2021). New attacks on Kubernetes via misconfigured Argo Workflows. https://www.intezer.com/blog/container-security/new-attacks-onkubernetes-via-misconfigured-argo-workflows/.

Ruan, P., Dinh, T. T. A., Loghin, D., Zhang, M., & Chen, G. (2022). *Blockchains: Decentralized and Verifiable Data Systems*. Springer.

Sabry, S. S., Kaittan, N. M., & Majeed, I. (2019). The road to the blockchain technology: Concept and types. *Periodicals of Engineering and Natural Sciences*, *7*, 1821–32.

Savelyev, A. (2017). Contract law 2.0: 'smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*, 116–34.

Scholliers, J., Permala, A., Toivonen, S., & Salmela, H. (2016). Improving the security of containers in port related supply chains. *Transportation research procedia*, *14*, 1374–83.

Scroxton, A. (2020). Cloud Snooper firewall bypass may be work of nation state. https://www.computerweekly.com/news/252479189/Cloud-Snooperfirewall-bypass-may-be-work-of-nation-state.

Shahrubudin, N., Lee, T. C., & Ramlan, R. (2019). An overview on 3D printing technology: Technological, materials, and applications. *Procedia Manufacturing*, *35*, 1286–96.

Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2020). A survey on physical unclonable function (PUF)-based security solutions for internet of things. *Computer Networks*, *183*, 107593.

Shepard, W. (2018). Meet the man fighting America's trade war against Chinese counterfeits (it's not Trump). https://www.forbes.com/sites/wadeshepard/2018/03/29/meetthe-man-fighting-americas-trade-war-against-chinese-counterfeits.

Sillaber, C., & Waltl, B. (2017). Life cycle of smart contracts in blockchain ecosystems. *Datenschutz und Datensicherheit*, *41*, 497–500.

Snowdon, A. W., Saunders, M., & Wright, A. (2021). Key characteristics of a fragile healthcare supply chain: Learning from a pandemic. *Healthcare quarterly (Toronto, Ont.)*, *24*, 36–43.

Staake, T., Thiesse, F., & Fleisch, E. (2005). Extending the EPC network: the potential of RFID in anti-counterfeiting. In *Proceedings of the 2005 ACM symposium on Applied computing* (pp. 1607–12).

Suh, G. E., & Devadas, S. (2007). Physical unclonable functions for device authentication and secret key generation. In *2007 44th ACM/IEEE Design Automation Conference* (pp. 9–14).

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*.

Tian, F. (2016). An agri-food supply chain traceability system for china based on RFID & blockchain technology. *International Conference on Service Systems and Service Management (ICSSSM)*, .

Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access*, *5*, 17465–77.

Treiblmaier, H., & Garaus, M. (2023). Using blockchain to signal quality in the food supply chain: The impact on consumer purchase intentions and the moderating effect of brand familiarity. *International Journal of Information Management*, *68*.

Urciuoli, L., Ma¨nnisto¨, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security– potential threats. *Information & Security: An International Journal*, *29*.

Verma, G. K., Singh, B., Kumar, N., & Chamola, V. (2019). CB-CAS: Certificate-based efficient signature scheme with compact aggregation for industrial Internet of Things environment. *IEEE Internet of Things Journal*, *7*, 2563–72.

Wang, L., Xu, L., Zheng, Z., Liu, S., Li, X., Cao, L., Li, J., & Sun, C. (2021). Smart contract-based agricultural food supply chain traceability. *IEEE Access*, *9*, 9296–307.

Weingartner, T., Batista, D., Kochli, S., & Voutat, G. (2021). Prototyping a smart contract based public procurement to fight corruption. *Computers*, *10*.

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*.

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN*, .
Xiujuan Wang, M. K. (2018). Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping. In *IEEE Intelligent Vehicles Symposium*. IEEE.

Yu, M.-D., Hiller, M., Delvaux, J., Sowell, R., Devadas, S., & Verbauwhede, I. (2016). A lockdown technique to prevent machine learning on PUFs for lightweight authentication.
IEEE Transactions on Multi-Scale Computing Systems, *2*, 146–59.