Global Supply Chains Security: A Comparative Analysis of Emerging Threats and Traceability Solutions

Abstract

- **Purpose:** The purpose of this study is to increase awareness of current supply chain security-related issues by providing an extensive analysis of existing supply chain security solutions and their limitations. The security of supply chains has received increasing attention from researchers, due to the emerging risks associated with their distributed nature. The increase in risk in supply chains comes from threats that are inherently similar regardless of the type of supply chain, thus, requiring similar defence mechanisms. Being able to identify the types of threats will help developers to build effective defences.
- **Methodology/approach:** In this work, we provide an analysis of the threats, possible attacks, and traceability solutions for supply chains, and highlight outstanding problems. Through a comprehensive literature review (2015-2021), we analyzed various supply chain security solutions, focusing on tracking solutions. In particular, we focus on three types of supply chains: digital, food, and pharmaceutical that are considered prime targets for cyberattacks. We introduce a systematic categorization of threats and discuss emerging solutions for prevention and mitigation.
- **Findings:** Our study shows that the current traceability solutions for supply chain systems do not offer a broadened security analysis and fail to provide extensive protection against cyberattacks. Furthermore, global supply chains face common challenges, as there are still unresolved issues, especially those related to the increasing supply chain complexity and interconnectivity, where cyberattacks are spread across suppliers.
- **Originality:** This is the first time that a systematic categorization of general threats for supply chain is made based on an existing threat model for hardware supply chain.

Keywords: Supply chain; Security; Threat Modelling; Traceability; Cyberattacks.

1 Introduction

1.1. Motivation

Global supply chain systems have become complex with several tiers, lawmakers, a growing number of companies, and buyers (Cui *et al.*, 2019). This complexity increases the challenges to protect the supply chain against security attacks (Zhang and Guin, 2020). Furthermore, due to the high number of involved entities in the supply chain, organizations may not be aware of the security level of the interconnected suppliers (Kieras *et al.*, 2021). Even though big companies can implement advanced security protections against security threats to protect their systems, to reach these organizations, the attackers can target their suppliers, which may have relatively less secure systems against cyberattacks (Kieras *et al.*, 2020). The attackers can exploit the intricate connections among the supply chain (SC) companies to hinder their efforts in providing secure and high quality-products (Aniello *et al.*, 2020). Successful cyberattacks can lead to catastrophic results in the SC system. For instance, in 2020, a major cyber incident occurred in SolarWinds company by injecting malicious code into its Orion management and monitoring software, which is supplied to numerous U.S. organizations and government agencies (Peisert *et al.*, 2021). SolarWinds' breach triggered more extensive SC cyber security

breaches in thousands of institutions, including Microsoft, Cisco, Intel and FireEye, which use SolarWinds' services compromised the attack (ENISA, 2021).

Due to the connected structure of SC systems, threats can affect a large number of organizations and result in severe effects on users and providers (Colicchia *et al.*, 2019). What makes this issue particularly challenging is the fact that the attackers can exploit SC threats at various SC stages. Therefore, assessing threats and vulnerabilities at every step of the chain is crucial against SC security threats (Zhang and Guin, 2020).

Several methods have been proposed in the literature to thwart existing threats in the SC. One of the most widely used countermeasures is implementing a tracking system, which provides assurance of the product's authenticity and enables counterfeiting detection (Cui *et al.*, 2019), (Aniello *et al.*, 2020), (Bocek *et al.*, 2017; Cao *et al.*, 2021; Caro *et al.*, 2018; Casino *et al.*, 2020; Cocco *et al.*, 2021; Ding *et al.*, 2020; Grecuccio *et al.*, 2020; Guin *et al.*, 2018; Islam *et al.*, 2018; Khan *et al.*, 2020; Kumar and Tripathi, 2019a; Liu *et al.*, 2021; Musamih *et al.*, 2021; Nazmul Islam and Kundu, 2019; Negka *et al.*, 2019; Tian, 2016, 2017a; Wang *et al.*, 2019; Xu *et al.*, 2019) . Tracking products over the SC process can allow product-related information to be available for SC companies. For example, tracking the products' movement from the initial process (e.g., raw material) to the end customer allows the organization to deliver the original product to the end customer. Therefore, this work focuses on the solution based on tracking the products over their entire lifetime.

Emerging technologies have been employed in tracking solutions, including blockchain (Cheung *et al.*, 2021; Leung and Chapman, 2020), physical unclonable function (PUF) (Cui *et al.*, 2019), (Negka *et al.*, 2019), smart contract (Guin *et al.*, 2018), and RFID (Raj *et al.*, 2019),(Badia-Melis *et al.*, 2015) to enhance the security of the SC process. However, implementing advanced technologies can increase the complexity in SC systems, requiring more attention on potential cyber threats (Xu *et al.*, 2019). Moreover, an attacker can target a system with sophisticated attacks by taking advantage of the security vulnerabilities of the used technologies in the SC solutions (Halak, 2021). Therefore, it is essential to conduct an extensive security analysis of the proposed SC solutions against potential threats to protect the SC system.

Although an important number of SC security solutions have been developed, only a few literature reviews provide SC security threat analysis. Hassija et al. (Hassija *et al.*, 2020) conducted a survey on SC application areas providing SC security threats and solutions. However, the study does not include a security threat analysis for SC systems or their security solutions, such as traceability solutions. Syed et al. (Syed *et al.*, 2022) studied a cyber security threat analysis on the component of traceability systems (e.g., the vulnerabilities of barcodes and RFID tags) with around one hundred relations, i.e., asset, threat, countermeasure relations. Although the study offers a threat analysis for the technologies implemented in the traceability solutions, it does not provide a security analysis of the overall SC system. Our work analyses the security of the different types of SC systems, i.e., electronic, food, and pharmaceutical SC systems. Moreover, we provide a comprehensive analysis of security solutions (i.e., traceability solutions), their limitations and future research opportunities. To the best of our knowledge, this is the first work on threat modelling of SC systems security.

To systematically address this goal, our approach was to:

- Analyze the existing body of literature between 2015 and 2021 related to supply chain security solutions. Given the immensity and heterogeneity of the supply chain

landscape, we decided to narrow down our focus to tracking solutions. These solutions have become pivotal in ensuring the security and integrity of supply chain operations. Within this framework, we prioritized three key types of supply chains, which are often the prime targets for security breaches: digital, food, and pharmaceutical supply chains.

- Extend the application of the CIST threat model, initially proposed for hardware supply chains, to various other supply chains. There are a few critical factors that have led to this decision. First and foremost, the inherent nature of threats in hardware supply chains is similar to general supply chain threats. The challenges posed by counterfeiting, information leakage, sabotage, and tampering are universal across various supply chains, regardless of the product type.

We perform this analysis by answering the following two primary questions (Qs):

Q1. How can a SC threat model be implemented to understand the potential threats and corresponding measurements?

Q2. What are the security solutions for SC traceability and the limitations of current studies?

The main contributions of this paper are listed as follow:

1. This paper presents a systematic security analysis for three types of SCs: electronic, food, and pharmaceutical. To systemically define the SC security threats, we adopt the CIST threat model (Halak, 2021), which is initially proposed for hardware SC. However, we show that it can be adopted for other types of SCs since the inherits of the SC threats are similar (e.g., counterfeiting, information leakage, sabotage, and tampering).
2. This paper provides a comprehensive summary of existing traceability solutions and an analysis of their limitations to outline the main outstanding security challenges and possible steps forward for securing SCs.

The paper is organized as follows. We introduce the CIST threat model in Section 3 and present a security analysis based on CIST for each analysed SCs. Section 4 introduces the existing SC tracking solutions for the analyzed SCs, briefly introducing the main used technologies. We perform an analysis of the limitations of current solutions in Section 5. We finally highlight the main research opportunities and discussion in SC security in Section 6 and conclude in Section 7.

2 Supply Chain Management and Traceability Solutions

Supply chain management (SCM) is the backbone of international trade. It ensures a seamless flow of goods and services from producers to consumers by weaving together a complex network of entities, both organizational and human (Croom, Romano and Giannakis, 2000).
SCM encompasses a broad range of topics, which are primarily divided into two categories: service supply chains and product supply chains (Hammi, Zeadally and Nebhen, 2023). Supply networks for products typically focus on physical goods (e.g., food supply chain (Moysiadis *et al.*, 2022)), starting with the acquisition of raw materials, going through multiple production stages, and culminating in the distribution of finished goods to customers. These supply chains often involve large inventories, logistical challenges with transportation, and issues with warehousing (Boyens *et al.*, 2021).

In contrast to product supply chains, service supply chains focus on providing intangible services. The goal of these chains is to ensure that the correct service is delivered to the right customer at the right time (Hammi, Zeadally and Nebhen, 2023). Human resources, task management, and real-time customer interaction are essential components of service supply chains. Due to the intangible nature of services, capacity management, demand forecasting, and quality assurance are of utmost importance. A comprehensive analytical framework can provide a deeper understanding of the broader SCM landscape, while the differences between product and service supply chains can help explain their respective dynamics.

For example, Croom et al., (Croom, Romano and Giannakis, 2000) introduce a novel framework to categorize and critically analyze existing literature in the field. Utilizing a two-dimensional matrix, they examined literature based on the level of supply chain analysis (from dyadic to network levels) and the element of exchange within the chain. The authors emphasized the need for multi-disciplinary approaches to address the complexities inherent in supply chain research comprehensively. The authors of (Spanaki, Karafili and Despoudi, 2022) provide an analysis and a framework for data in the SC and how to ensure the data quality during information sharing in the SC regarding the context and infrastructure. Another work proposed by Storey et al., (Storey *et al.*, 2006) where they analyzed six supply chains that involved 72 European companies to evaluate the state of supply management today comprehensively. The study discovered that there is a significant gap between current theoretical frameworks and actual supply management practices. Most practitioners fail to exert full influence throughout the supply chain. It offers valuable insights into the difficulties and potential of supply chain management as a profession and a field of study.

Furthermore, integration of tracking technologies is becoming a crucial organizational strategy as SCM complexity increases. Tracking technologies provide detailed visibility into the movement of commodities throughout the product supply chain, from sourcing raw materials to delivering goods to the end consumer (Aniello *et al.*, 2020). Monitoring this movement helps avoid bottlenecks, maximize inventory levels, and ensure on-time deliveries.

Moreover, tracking solutions stand out as critical enablers as SCM evolves to address global challenges—like ensuring sustainability, meeting regulatory compliances, or navigating geopolitical disruptions. Additionally, advanced monitoring technologies like blockchain and IoT enhance supply chain efficiency and dependability and promote accountability and traceability as core SCM principles (Moysiadis *et al.*, 2022). However, with the adoption of these digital advancements, the exposure to cyber threats becomes more pronounced, necessitating robust security measures. These threats can manifest in various forms, including data leaks, business operation disruptions, and reputation damage. Recent researches emphasize the urgent need for a strong cyber security and threat management strategy in traceability systems. This is crucial not only for safeguarding business assets but also for maintaining the integrity and dependability of the entire supply chain. For example, Syed et al., (Syed *et al.*, 2022) propose an extensive assessment of threat modelling, which aims to assist stakeholders in identifying and resolving potential vulnerabilities that may arise while incorporating technological solutions for traceability. The report's approach is systematic and comprehensive, highlighting over a hundred relationships between assets, threats, and countermeasures relevant to supply chain traceability. The paper focuses on conducting threat

modelling for technologies used in supply chain tracking solutions but does not address the threats that target the supply chain as a network.

While our primary focus has been on traceability in supply chains, it's noteworthy that threat modelling has broad applications across various fields, emphasizing its critical nature. For instance, recent advancements in threat modelling have been tailored to hybrid/smart systems, integrating physical, human, and cyber aspects to ensure robust security in intricate setups (Valenza *et al.*, 2022). These diverse applications further underscore the importance of comprehensive threat analysis and management in any domain.

This work discusses security threats in different supply chains and highlights the importance of understanding these risks to safeguard the integrity of product and service supply chains. Additionally, we provide a comprehensive review of advanced tracking solutions that improve supply chain visibility and critically evaluate their limitations, providing a balanced perspective on their role in enhancing supply chain resilience and efficiency.

3 Supply Chain Threat Modelling based on CIST

Knowing the various threats of a system is essential to protect such a system. Threat models allow to represent, identify, and reason with the various threats. In this section, we will first introduce CIST, a hardware SC threat model, then we will show how CIST is used to analyse the cyber security threats of three different SC systems.

3.1 CIST threat model

Threat modelling allows the analysts to identify potential threats in the systems. After determining the system threats, they can build an effective security mechanism based on the threat analysis. There are different types of threat models available such as Trike (Saitta *et al.*, 2005), P.A.S.T.A (Simopoulos *et al.*, 2021), DREAD (Ram and Pant, 2010), STRIDE (Sancho *et al.*, 2020). The choice of which model to use depends on the challenges of the analysed system. The threat model for SC systems may require more specific categorization, such as *counterfeiting* and *sabotage* due to the nature of SC threats.

In this study, we used the CIST threat model (Halak, 2021). CIST is a threat model for hardware SC systems, which consider the threats from the first design step to the discarded integrated circuits (ICs) recycling phase. Given that the nature of hardware SC threats is similar to the general SC threats, this threat model is amenable to cover other types of SCs.

In the following subsection, we present how CIST can be easily used to model threats for three different SC systems. The CIST model defines threats in four categories counterfeiting, information leakage, tampering, and sabotage (Halak, 2021). All of these categories allow representing the various threats of different SC systems. We introduce below each of the categories in detail.

Counterfeiting: The purpose of this threat is to produce and distribute fake products.

Information Leakage: The attacker aims to reveal the system's secret or product design. This secret can be the entity credentials, secret key, design information of a product, or any other information useful for the attackers.

Sabotage: Products over any stage of the SC can be sabotaged in different ways to damage the production process or the product itself.

Tampering: This threat targets the integrity of the system. By tampering with the product, an attacker can cause faulty behaviour in the system process, such as obtaining the sensitive information stored in the product.

3.2 Cyber Supply Chain Threat Modelling based on CIST

Through threat modelling, we can provide an abstraction of the analysed system, where especially for SC, the types of threats are related to the system's nature. In this section we show how the CIST threat model can be applied in three different SC scenarios with different natures, including digital, food, and pharmaceutical SCs. Together with each threat, we will introduce the corresponding countermeasures.

3.2.1 Digital Supply Chain Threat Modelling and Countermeasures

The rapid development of advanced technologies has brought tremendous demand for electronic components, resulting in an increase in cyberattacks against hardware surfaces. The security of the hardware products has gained increasing attention from daily electronic products including smartphones, PCs, smart cars to more critical infrastructure such as satellite communication, electrical grids. Using the high number of electronic products in the entities' systems may result in a complex SC network where critical potential threats occur.

For the digital SC, we start by analysing the various stages of the production process (from the beginning until the end customer stage) as illustrated in Figure 1. IC production starts with the intellectual properties (IP) design stages, where third-party vendors provide sourcing (IP) designs. In the second stage, the system integrator generates the layout files. After the third stage, where foundries fabricate integrated circuits, testing and packaging these circuits occur in the fourth stage. The next stage is customer usage of the final products. Finally, the IC products which have completed their lifecycle are discarded by their users.

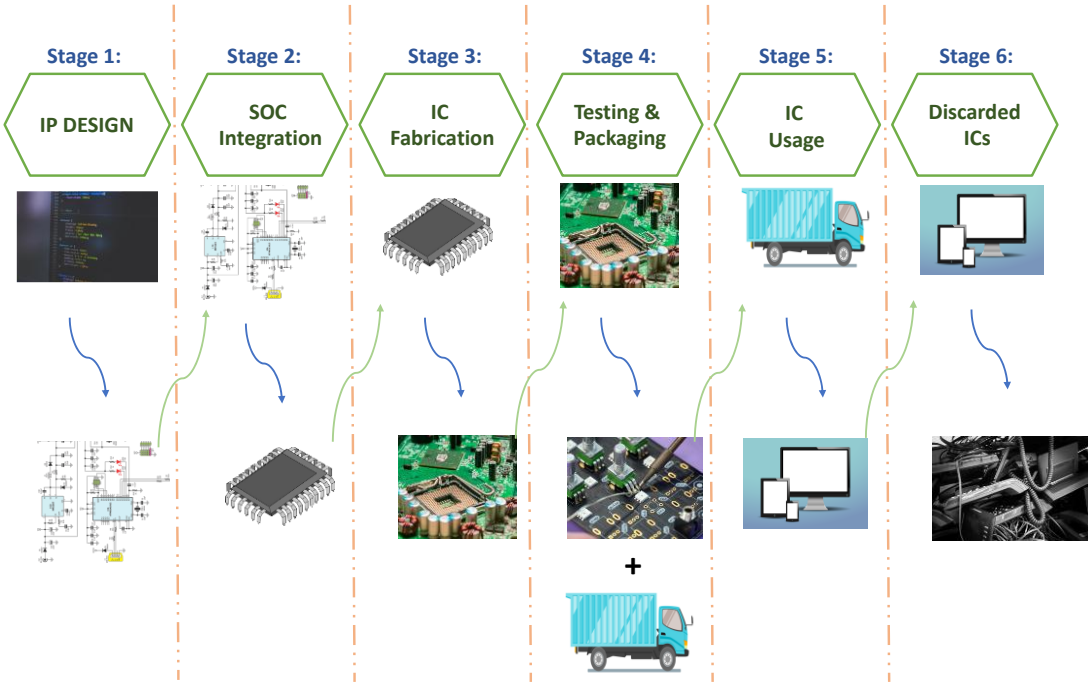

Figure 1 Schematic of the digital SC

In Table 1, we provide all these stages and the associated threats. Together with each threat, we show the affected security properties and what kind of impact would these threats have if

exploited by an attacker. These threats usually go from economic impact to reputation losses (which can be translated into economic impact) to system design undermining. Let us introduce our threat analysis based on CIST and provide the countermeasures for each category.

A) Counterfeiting

Counterfeiting threat is one of the most critical threats during electronics production and delivery. An attacker can imitate the authentic electronic products design and produce counterfeit ones. Counterfeit products can be remarked, overproduced, cloned or recycled devices (Xu *et al.*, 2019). The attacker can relabel the used components and sell them, if the counterfeited devices are not detected during this process. Untrusted fabrication foundries can produce more electronic devices than the contract indicates among the suppliers and sell them using primary or secondary markets.

There are several *countermeasures* for detecting and avoiding counterfeited electronics. For example, some ways to detect counterfeited electrical chips are physical tests, including external visual inspection (EVI), scanning acoustic microscopy (SAM), and x-ray fluorescence (XRF) spectroscopy. Moreover, electrical tests on the chips can detect the forged device in the SC (Yang *et al.*, 2017). To avoid counterfeited electronics, the countermeasures should be applied at all stages of the SC. The execution of the proposed tests/checks is highly challenging for companies in terms of implementation complexity and costs. A cheaper and less complex

Type of SC	CIST	Affected Security Property	Attack Examples	Stage	Potential Impact
Digital Supply Chain	Counterfeiting	Authenticity	Cloning ICs	Stage 1: IP design Stage 2: SoC Integration Stage 3: IC Fabrication Stage 4: Testing & Packaging Stage 6: Discarded ICs	Financial losses. Loss of company reputation. Untested chips can cause a security risk to the system.
			Remarking ICs	Stage 3: IC Fabrication Stage 4: Testing & Packaging Stage 6: Discarded ICs	
			IC Overproduction	Stage 3: IC Fabrication	
	Information Leakage	Confidentiality	IP Privacy	Stage 2: SoC Integration Stage 3: IC Fabrication	Financial losses: if the products' design IP is disclosed.
			Data Theft	Stage 5: IC Usage	
	Sabotage	Availability	Stuxnet-Type Attacks	Stage 5: IC Usage	Financial losses and negative effects on company reputation due to SC system failure.
			Clkscrea		
			Rowhammer		
	Tampering	Integrity	Hardware Trojan	Stage 2: SoC Integration	Undermining the design integrity.

Table 1 CIST threat modelling examples for the digital SC stages adopted from [32].

alternative to such countermeasures is to track the electronic product in the trusted network. This solution is highly used to prevent potential counterfeiting infiltration to the SC since the organization can trace each movement of the products over the chain (Kulkarni *et al.*, 2019; Yang *et al.*, 2015, 2017).

B) Information Leakage

Information leakage threats in digital SC consist of all types of information that can be the target of the attackers at any stage of the SC. The data can be of different types, e.g., product design information, suppliers' sensitive data, logistics, or the data stored in the electronic device. For example, the design secret of electronics can be disclosed by an attacker to produce new counterfeited products. Another attack goal is to steal the information inside the chip after its deployment. The attacker might use different techniques for information leakages, such as a memory attack to steal sensitive information from memory, or a PUF modelling attack using a machine learning attack to model the PUF's CRPs (challenges and responses).

The *countermeasures* for information leakage in the digital SC are various and depend on the information that needs to be protected. In case the main target of an attacker is the sensitive data stored in the electronic product, then protecting the physical components from unauthorized access or modification can prevent the information disclosure. Other countermeasures consist of implementing strong encryption over the communication channels of the SC in order to protect the companies' and products' information (Litke *et al.*, 2019). Countermeasures that deal with the stealing of information inside the chip include side-channel analysis, cache timing and speculative execution attacks (Halak, 2021).

C) Sabotage

Sabotage threats in digital SC generally deal with threats exploited by the attacker to damage the product, a process, or the entire SC. For instance, in case the attacker's purpose is to damage the ICs (that can cause a delay in the supply process), then the attacked company can spread the sabotage attack/damages to other entities involved in other phases of the SC.

Countermeasures should be put in place not only by the targeted company but also by the interconnected suppliers. The primary countermeasure is to perform a risk analysis. Analysing and ensuring the system security requirements, identifying and preventing possible vulnerabilities, and thorough risk analysis can help protect the system against sabotage attacks.

D) Tampering

Tampering threats in SC exploit the interdependent nature of digital SC. For example, to steal information stored in an electronic product such as encryption keys (e.g., through an information leakage attack), the attacker first tampers the electronics to unauthorize changes in the stored data. Through tampering, the attacker can cause faulty behaviour in the hardware products in different stages of the chain (Halak, 2021).

Countermeasures against tampering for digital SC are the general countermeasures deployed against such threats. Analysing the possible tampering attacks, such as trojan insertion or fault injection to the hardware device, is an effective countermeasure. Another countermeasure is to apply tamper-resistant techniques before developing electronic products (Halak, 2021).

3.2.2 Food Supply Chain Threat Modelling and Countermeasures

The food SC's nature can be slightly different from the digital SC, where external conditions (e.g., room temperature, humidity) have high importance on product quality. Therefore, even though the SC threats are similar for the overall systems, the way how these threats occur in specific SCs (e.g., digital SC and food SC) can be different. The production chain of the food SC can be slightly different from the digital SC in terms of product type and manufacturing

process. As shown in Figure 2, the initial step is harvesting and manufacturing the end product. The next step occurs at the warehouse by storing the final product to send suppliers. The third stage is the delivery of final products to the buyer. The final will be the selling process by retailers and customer usage.

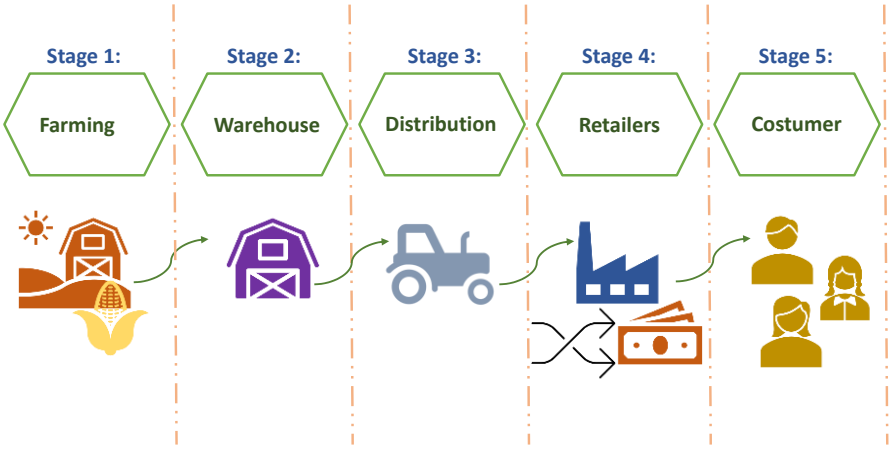

Figure 2 Schematic of the food SC

In Table 2, we introduce all the stages of the food production process (from the beginning until the end customer stage), their associated threats, attack examples and the potential impact these threats have on the food SC.

Let us now introduce the analysis we performed on the threats of the food SC using CIST, where we categorized the threats using the CIST categories and provide each category with the possible countermeasures.

A) Counterfeiting

Counterfeiting threat is a critical threat in the food SC, as counterfeited or contaminated food products can cause serious damages, like severe side effects for the consumers' health that in some cases can also bring to death (Mäde *et al.*, 2013). The adversary's goals through food counterfeiting or contamination are to cause illness of the food consumers and damage the company's reputation. Another threat in the food SC is the counterfeiting of electronic devices. In particular, logistic companies (part of the SC) may need to attach electronic devices to the food containers in order to control external conditions (e.g., room temperature, humidity) or track the products over the supplier process. If a significant amount of the electronic devices attached to food containers are counterfeited, then they will not be able to properly track the container or its conditions, with negative consequences, like loss/damage of the products or trust issues among suppliers.

The main *countermeasure* against counterfeiting is to use technologies that allow food tracking in the SC. For tracking purposes, electronic components such as RFID, temperature, or humidity sensor are used (Bibi *et al.*, 2017). To protect the system against cyberattacks, also

Type of SC	CIST	Affected Security Property	Attack Examples	Stage	Potential Impact
Food Supply Chain	Counterfeiting	Authenticity	Food contamination with foreign objects	Stage 1: Farming/Production Stage 2: Warehouse Stage 3: Distribution Stage 4: Retailers	Hazardous consequence on public health. Loss of company reputation and advantage on company's superiority against the competitors.
	Information Leakage	Confidentiality	Data Theft	Stage 1: Production	Loss of IP, e.g., the formula information of food products can be disclosed. Financial losses.
	Sabotage	Availability	Cyberattacks on production facilities	Stage 1: Production	Bypass of organization's security mechanisms. The attacker can cause a failure in the organization system, triggering the loss of company reputation. Loss of reputation.
	Tampering	Integrity	Fault injection attack to attached electronics of drugs' containers	Stage 2: Warehouse	The attackers can tamper with the electronic products controlling the external factor for the drug quality, resulting in loss of company reputation and financial losses.

Table 2 CIST threat modelling examples for the food SC stages.

these electronics' security should be protected (Costa *et al.*, 2013).

B) Information Leakage

The attacker can exploit the information leakage threat in the production stage to steal the secret product formula, which would bring in losing the competitive advantage that a company has with respect to the competitors. Information is of high importance for organizations, thus, protecting information (related to the company's competitive advantage and its products), is critical for all SC organizations. Moreover, the attackers may aim to steal information about the supply process to sabotage the SC flow using physical or cyberattacks. A successful attack against the SC can cause a delay, which can affect the food products' condition, such as freshness, and can result in loss of the supplier trust against the buyer companies.

Several *countermeasures* can be put in place to protect information related to products, organizations, and their interconnected suppliers. The countermeasures applied for food SC are similar to SCs countermeasures for information leakage, like secure communication, secure/encrypted data storage, data access control. In particular, an attacker targets the company in several ways to steal the secret product formula. However, companies can protect their information by understanding the potential vulnerabilities that the attacker can exploit. Implementing strong encryption is one of the main techniques against information disclosure. Companies can define the information policies and the access privileges against unauthorised alteration of the stored data. To protect information related to the SC tracking process, companies can implement blockchain technologies. One of the main features of the blockchain is decentralization, providing robustness and reliability for the system.

C) Sabotage

Sabotage threats for the food SCs mainly try to attack the electronic devices that control the food quality, e.g., devices that monitor the storage temperature, moisture, delay in transportation. Another threat would be to sabotage the manufacturing devices that are employed during the food SC. Given the high sensitivity of the products, even a small alteration in the production and product life cycle can have serious negative consequences on the product and the entire SC.

The main *countermeasures* against sabotaging threats are protection mechanisms against cyber threats, such as malware attacks. Analysing potential sabotage attacks and consequently updating the system defence mechanisms can help in reducing such risks (Ahmed *et al.*, 2020). If the system implements electronics to track food products or control food containers' conditions, the attacker can target the SC process for physical sabotage. In such cases, SC entities can implement an authorisation mechanism to reach the electronic devices physically.

D) Tampering

For the food SC, an attacker can *tamper* the products by injecting foreign objects (e.g., clenbuterol, Sudan red and melamine (Kamath, 2018)) or causing damage to the electronic devices of food containers that control internal and external conditions.

Countermeasures for the tampering threats for the food SC depend on the type of threat. To prevent the tampering of the food product itself, the attacker requires physical access to the food. This threat can be prevented by applying an authorization mechanism, e.g., to the electronic devices used to track the conditions or positions of the food containers. In this case, techniques like a blockchain-based authentication system that reads RFID data can be used (Mondal *et al.*, 2019). The usage of an authentication control system ensures that only trusted users have access to the electronics.

3.2.3 Pharmaceutical Supply Chain Threat Modelling and Countermeasures

In this section we analyse pharmaceutical SC threats using the CIST threat model. In Table 3, we show the various stages of the pharmaceutical SC with their associated threats, possible attacks, and the impact of these threats on the SC.

This SC production process has some similarities with the food SC as shown in Figure 3, but it is more critical since detecting faulty products in the food SC is more straightforward than the pharmaceutical SC that might take months, even years to identify pharmaceutical faulty products.

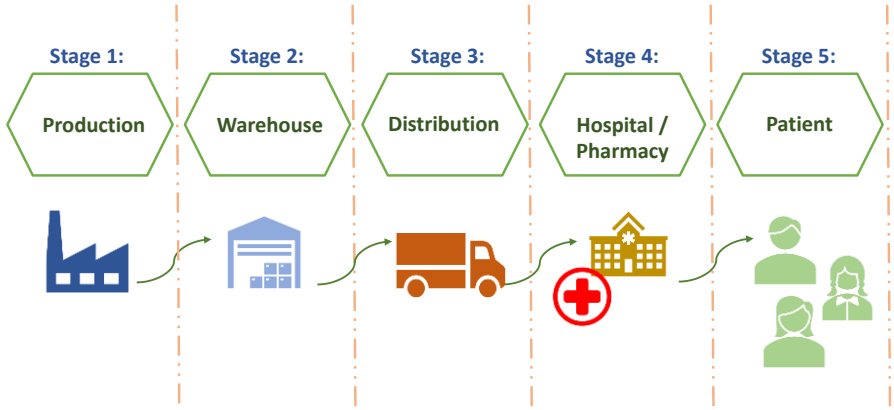

Figure 3 Schematic of the pharmaceutical SC

A) Counterfeiting

Counterfeiting is a severe *threat* for pharmaceutical SCs, as counterfeited products pose a serious health risk to the users.

Table 3 CIST threat modelling examples for the pharmaceutical SC stages.

Type of SC	CIST	Affected Security Property	Attack Examples	Stage	Potential Impact
Pharmaceutical SC	Counterfeiting	Authenticity	Fake drug product (i.e., the ones which have different ingredients from the original formula)	Stage 1: Production Stage 2: Warehouse Stage 3: Distribution Stage 4: Hospital/Pharmacy	Hazardous consequence on public health. Loss of company's reputation and advantage against the competitors.
	Information Leakage	Confidentiality	Data Theft	Stage 1: Production	Financial losses: as the formula information of drugs can be disclosed.
	Sabotage	Availability	Cyberattacks on production facilities	Stage 1: Production	Bypass of organization's security mechanisms. The attacker can cause a failure in the organization system, triggering the loss of company's reputation.
	Tampering	Integrity	Fault injection attack to attached electronics of drugs' containers	Stage 2: Warehouse Stage 3: Distribution	Tampering the electronic products that control the external factor for the drug quality.

One of the main *countermeasures* for counterfeiting is to use tracking solutions, e.g., by tracking every single package over the SC (Abbas *et al.*, 2020; Ahmadi *et al.*, 2020; Sinclair *et al.*, 2019; Sunny *et al.*, 2020). To mitigate/prevent counterfeiting in the pharmaceutical SC, we can use similar countermeasures to the ones introduced in Sections 3.2.1 and 3.2.2.

B) Information Leakage

The main goal of the *information leakage* threats in the pharmaceutical SC is to steal the drug formula or design, which can occur through insider attackers or cyberattacks. The impact is similar to those mentioned in the previous SCs, i.e., economic losses.

Similar *countermeasures* to the ones proposed in the previous SCs are applied for the pharmaceutical SC against information leakage, like secure communication, data access control, secure data storage. A risk analysis should be performed to understand the ways the attacker reaches the design information, and further specific countermeasures should be put in place.

C) Sabotage

The main *sabotage threats* for the pharmaceutical SC are conducted in the production and transportation phase. Since the nature of drugs requires specific conditions (e.g., low storage temperature), the attacker can aim to undermine them. For example, if the company does not determine a secure access control system for accessing the electronics that control these external conditions, the insider threat actor can exploit them to sabotage the product.

Understanding the pharmaceutical SC threats is essential to provide efficient *countermeasures* for the sabotage threats. These threats can occur in several ways, i.e., the attacker can sabotage the electronics that control the external factors (needed for drug quality), products, and the production process. It is essential to identify the system vulnerabilities and the ways the attacker can sabotage the system. As mentioned previously, security analysis needs to be conducted to protect the system against cyberattacks and insider attackers. It is essential to put in place access control measures for the physical and cyber access of electronics and products.

D) Tampering

In pharmaceutical SC, the tampering *threats* are critical as they can cause critical consequences for both organizations and people. For example, some medications like the Covid-19 vaccine (e.g., Pfizer-BioNTech vaccine (James, 2021)) needs to be transported in an extreme cold-storage condition between −80°C and −60°C. If the attacker tampers with electronics that control the temperature of the products, then the supply process is postponed or, more seriously, collapses.

The tampering threat's main *countermeasures* are similar to those mentioned in Section 3.2.2, e.g., users' access can be controlled by an authorization mechanism so that only approved users can access and modify the attached electronic products.

4 Supply Chain Security Tracking Solutions

Let us introduce the main solutions for ensuring the security of SCs. In particular, we will focus on the traceability solutions for the three analysed SCs, i.e., electronic, food and pharmaceutical. For a detailed summary of the tracking solutions their used technologies, advantages and disadvantages check Table 5, in the Appendix.

4.1 Electronic Supply Chain Tracking Solutions

The main existing tracking solutions use technologies like authentication mechanisms, blockchains, PUFs, and a mixture of blockchains and PUF. In particular, the work in (Guin *et al.*, 2018) presents a tracking solution for IoT edge devices. The proposed solution employs device authentication by using Static Random-Access Memory–based (SRAM-based) physically unclonable functions. In case the attacker can infiltrate the cloned products in the SC, the fake IoT edge devices are detected using periodic authentication mechanisms.

Another technique is to use blockchain-based applications to record the ownership of electronic devices. In (Islam *et al.*, 2018), PUF technology is employed in the manufacturing process to produce a unique ID for each IC component. The PUF's CRPs are stored in the blockchain system, and every manufacturer registers the system with the generated PUF-based unique ID. In this way, SC organizations can track the IC components and authenticate them using a unique ID stored in the blockchain. Similarly, in (Negka *et al.*, 2019) is introduced a system that identifies each component through the SC using the blockchain technology (in particular, Ethereum) and PUFs, to prevent counterfeits. This work shows the cost information for contract deployment but fails to provide further explanations on how PUFs and Smart Contracts are employed. Therefore, the way of implementing those technologies can result in a high per-transaction cost which may have a reverse effect on the system's practicality. Another solution based on blockchain focuses on tracking all the components circulating in the SC, e.g., chips (Cui *et al.*, 2019). This solution proposes to perform the tracking of the devices in the digital SC through their authentication. An anti-counterfeiting tracking solution for the digital SC based on the blockchain and PUF technologies is introduced in (Aniello *et al.*, 2020), where PUF and smart contracts are used.

A blockchain-based certificate authority framework is proposed in (Nazmul Islam and Kundu, 2019) to manage curial chip information (e.g., electronic chip identification, chip grade, and transaction time). The silicon PUFs are applied in the form of NFC (Near Field Communication) for the authentication process, which is launched through a software application, e.g., a mobile application. Although the system uses a PUF-based authentication process against counterfeiting attacks, the mobile authentication system may cause a vital security risk such as human error, information leakage, or other security vulnerabilities. Another solution based on blockchain certificate authority is introduced in (Xu *et al.*, 2019), where the proposed framework ensures the integrity of the digital SCs. This framework allows to manage the information of the chips and can mitigate four common digital SC threats, including recycling, remarking, cloning and overproduction.

A double-layer framework[1] for the traceability of the SC is proposed in (Ding *et al.*, 2020), where better scalability and performance is offered. However, the proposed multi-blockchain framework results in a high-cost transaction, leading to implementation and adaptation problems for the entities. A solution for tracing the reverse logistic process of mobile phones that uses smart contracts technologies is introduced in (Dasaklis *et al.*, 2019). The implementation of the proposed architecture has several barriers to its adoption in the reverse

[1] A double-layer framework for blockchain-based solutions implements several types of blockchain technologies such as consortium, public and private blockchain.

SC (i.e., technological, legal, financial/economical, market-oriented), and its interaction with the stakeholders is missing.

4.2 Food Supply Chain Tracking Solutions

Recently, novel solutions have been employed for food SC to provide transparency, traceability, reliability and improve food quality and safety. In this section, we will provide some of the most prominent solutions that mainly focus on the traceability aspects.

A traceability system for agri-food SCs based on RFID and blockchain technology used to enhance the safety and quality of the Chinese agri-food markets is presented in (Tian, 2016). The proposed framework implements RFID technology to track food products and stores their related information in the blockchain. In (Tian, 2017a) is introduced a conceptual model for the traceability of the food SC based on HACCP (Hazard Analysis and Critical Control Points), where the SC process is introduced with different application scenarios, i.e., production link, processing link, warehousing management link, cold chain distribution link, retailer link.

Another work that presents an agri-food SC traceability solution, called AgriBlockIoT, is introduced in (Caro *et al.*, 2018). AgriBlockIoT is based on blockchain technologies and offers transparency and immutability of the stored data. Furthermore, the edge devices (i.e., gateways and mini-PC) are used as full nodes of the layered blockchain where the network robustness is enhanced.

Similarly, Wang et al. (Wang *et al.*, 2019) propose a tracking system based on the Ethereum blockchain, where all the product information and transaction histories are permanently recorded using smart contracts. This solution provides a user-friendly web page interface and provides the detailed costs of using the smart contract deployment for raw materials.

Other traceability solutions were proposed for specific food SCs such as cacao and soybeans (Salah *et al.*, 2019), eggs (Bumblauskas *et al.*, 2020), agri-food (Hayati and Gusti Bagus Baskara Nugraha, 2018; Kim *et al.*, 2019; Lin *et al.*, 2018). A blockchain-based framework is used to improve the tracking system's trust and resilience for the dairy sector (Casino *et al.*, 2020). Smart contract technologies are used in the study to provide a transparent and tamper-proof solution. IoT devices that can interact directly with the blockchain are used to receive data, such as the products' temperature. Although the study claims that the security and privacy of the system are ensured, the IoT devices may become vulnerable, i.e., advanced cryptography algorithms cannot be applied due to memory capacity and limited code space (Casino *et al.*, 2020) (Garg *et al.*, 2020). Thus, a security analysis of the proposed framework is needed to detect the various system vulnerabilities.

4.3 Pharmaceutical Supply Chain Tracking Solutions

Given the high complexity of SC networks, if the attacker finds a way to introduce the fake product to the SC systems, especially the pharmaceutical SC, the consequences can be dangerous for human health (Chien *et al.*, 2020). The Drug Supply Chain Security Act (DSCSA) provides protection requirements to clarify the regulations against the contamination of drugs. Under the DSCSA, a system tracking should be provided from start to end for the drugs SC. Thus, various solutions for drugs security have been proposed that use similar techniques to what we have explored in the previous sections.

A solution based on blockchain technology that ensures data immutability is introduced in (Bocek *et al.*, 2017). This solution, called Modum.io AG, implements the smart contract technology to share the product's information (e.g., temperature) that is provided by IoT

Testing Technique	Detection Level	Cost
In-Circuit Testing	Can determine only Trojans that temper tested nodes	≈ $20k+
Functional Testing	Can determine only Trojans that temper tested board function	≈$50k+
Bare-board Testing	It may not be very effective to detect Trojans	≈$2k+
Visual Inspection	Can determine potential Trojans in the system when multiple imaging modalities are applied	≈$12k+

Table 4 PCB testing to detect tampered hardware (adapted from [66]])

sensors used to maintain the quality of the product. Another blockchain-based solution that works towards meeting the regulations enforced by the DSCSA is proposed in (Sinclair *et al.*, 2019).

A distributed application (DApp) based on blockchain to avoid a mismatch of data with RFID tags, used for tracking, is introduced in (Sylim *et al.*, 2018). DApp detects malicious attempts in terms of malicious injection by checking data stored in the file system. Another blockchain-based solution (Kumar and Tripathi, 2019b) is based on certificate authority for goods transactions where the entities' trust is required for the product security to protect against the action of attackers. Gcoin blockchain was used in (Tseng *et al.*, 2018) to provide transaction transparency of drugs in the SC. A solution that ensures anti-tampering and high transparency of the information used in the system of product recall service is introduced in (Wu and Lin, 2019).

5 Analysis of the Limitations of Existing SC Tracking Security Solutions

Due to the complexity of today's SC network, their security solutions comprise a limited part of the security of the companies and their products. Although existing solutions provide an important contribution to SC security, attackers can still exploit unexpected vulnerabilities. Therefore, the security analysis of the SC security solutions should be extended and performed for all types of SCs. In this section, we will provide the limitations of the existing SC tracking solutions.

The first limitation deals with contract manufacturers (CM), in particular, malicious CM and the vulnerabilities and limitations introduced by them.-In the framework introduced in (Cui *et al.*, 2019), the security threats are analysed regarding trusted CM. The adversary manufacturer may target the big companies through their suppliers, as SC is a vast multi-supplier network. The malicious CM can generate an authentic ID for the malicious devices. In this case, the system will not recognize any anomalies as the system trusts the CM. For this type of threat, (Cui *et al.*, 2019) proposed that the buyer organization implement an additional verification process to guarantee products security. However, this may not be a cost-effective strategy if extra security tests are needed. To avoid such extra costs, companies can choose to trust the manufacturer. Trusting suppliers without additional security tests on the provided products can have negative effects on the company in case the counterfeited chips are used. An example of such an attack occurred in 2018 called “Big Hack” (Businessweek, 2018). The attack targeted

a Chinese motherboards company called Super Micro Computer Inc. (Supermicro) and fake chips were attached to the produced motherboards, allowing a backdoor for malicious actors. The result was catastrophic for Supermicro's stocks which were affected by a 41% decrease (Mehta *et al.*, 2020) and according to Bloomberg Businessweek 30 U.S. companies could be affected by this attack, where they might not detect anomalies on chips as soon as the attack started. Additional PCB (Printed Circuit Board) testing methods to detect tampered hardware can be introduced, but the cost of external tests can be expensive for companies, as indicated in Table 4. Thus, companies may choose to trust manufacturers to reduce extra expenses, which can cause further vulnerabilities in the system.

The second limitation deals with the costs associated with the use of private blockchain networks, such as Ethereum, where the total cost for storing and managing the data can be high. Although private blockchain can provide a secure transaction (e.g., private blockchain only allows the authenticated user where the users should have permission to make changes in the system), the cost for the overall system may not be practical for companies due to the per-transaction cost. These studies (Caro *et al.*, 2018), (Salah *et al.*, 2019), (Kim *et al.*, 2018), (Sylim *et al.*, 2018) employ private blockchain but do not provide a cost analysis for the proposed solutions, but is expected to result in a high implementation cost.

The other limitation deals with the authentication mechanisms of the products. There exist solutions that use authentication mechanisms for product verification, e.g., the solution introduced in (Zhang and Guin, 2020) performs an attack analysis and uses two-step authentication. In the first authentication step, the ECID (electronic chip ID) stored in the RFID is checked to match the chip's *ECID (i.e., *ECID is the ID given by product foundry for physical identity). If the first step fails, then the second step does not proceed. In this case, the ECID can be cloned or tampered with to manipulate the original product authentication (Guin *et al.*, 2014). If the attacker manages to tamper enough product IDs, the system assumes that the products are counterfeited, even though they are produced by trusted companies with original product IDs. This attack may damage the supplier's reputation and cause costs and time losses. If the authentication fails, the system integrator can contact the distributor and either trust or reject the chips. Rejecting or re-testing the chips results in economic losses for the supplier company and time loss for the buyer.

Limitations also exist for authentication mechanisms that use the PUF technology, where these limitations mainly deal with storing problems and their security issues. In (Xu *et al.*, 2019) is proposed a security analysis for threats such as recycling, overproduction and cloning, that carries several limitations for the authentication mechanism. Given the difficulties in storing the vast amount of PUF's CRPs and the reliability concerns for PUFs under external environmental conditions, the PUF model is stored in the IP owners' database. The attacker can find a way to reach this database and steal the PUF model, thus, can produce cloned chips. Moreover, the attacker can use reverse engineering or machine learning algorithms to produce original challenge-response pair from the stored PUF model (Polypufs *et al.*, 2019).

Another limitation of current SC security solutions deals with the data storage component. In (Patil *et al.*, 2018) is proposed a security framework based on blockchain technology for smart greenhouse farming, where cloud storage is used for the data of the greenhouse devices. Cloud storage is a centralized network that suffers from security vulnerabilities, such as unauthorized

access to the management interface (Grobauer *et al.*, 2011), single points of failure and data integrity.

Overall, the main limitations are due to the use of external technologies, like IoT devices, RFID technologies, QR codes, and the limitations and vulnerabilities that come with them. The use of IoT technologies, such as sensors for controlling food quality or RFID for reading the information, bring limitations as they might cause important security vulnerabilities, especially if a security analysis is not performed to mitigate and prevent potential threats against these devices. IoT devices might not provide strong guarantees for system security due to their limited nature, such as low storage capacity for advanced security protection methods. Thus, the attacker may exploit these devices to sabotage the system.

A solution based on IoT technology for the food SC is provided in (Casino *et al.*, 2020) together with limited security analysis. IoT technology is also used in the pharmaceutical SC. For example, in (Ahmadi *et al.*, 2020) is proposed an IoT-based tracking solutions to prevent counterfeited drugs. However, this work fails to provide any security analysis for the proposed IoT-based solution. Similarly, a blockchain-based traceability solution for the pharmaceutical SC is proposed in (Kumar and Tripathi, 2019b), where the solution uses encrypted QR codes to store details of the medicine. However, the integrity of the information can be threatened by impersonation attacks, and the QR code can be copied or altered to sabotage the system.

In (Raj *et al.*, 2019) is introduced another blockchain-based pharmaceutical SC solution that uses unique EPC (Electronic Product Code) to perform the products' authentication using RFID. However, the RFID technology brings new vulnerabilities (Tieyan and Robert, 2007), and further attacks can be performed on them (Xiao *et al.*, 2009), e.g., if the attacker can copy or manipulate the RFID tag, then he can sabotage the system.

Other limitations deal with the lack of threat analysis of the implemented security solutions for SC traceability. The usage of blockchain provides secure solutions as long as the used components/techniques, e.g., IoT devices, RFID, are secure as well. A good part of existing solution fail to provide a security analysis and the risk factors (Ahmadi *et al.*, 2020), (Tian, 2017b), [26], [41], [55], (Kim *et al.*, 2018), (Negka *et al.*, 2019), (Bumblauskas *et al.*, 2020), (Bocek *et al.*, 2017), or provide a very limited security analysis (Zhang and Guin, 2020), (Dasaklis *et al.*, 2019), (Mondal *et al.*, 2019), (Wang *et al.*, 2019) on how the system can prevent or mitigate SC threats. Given the complexity of the SC systems and the heterogeneity of the implemented solutions, cyber threats can be exploited from any vulnerable point of the system and can cause negative consequences.

6 Discussion and Future Direction

Supply chain security has received increasing attention in the literature. Understanding the SC security threats, challenges, and requirements is critical in protecting the SC systems against security attacks. At the beginning of the study, we posed two primary research questions that we answered in this paper. The first question (Q1) is "*How can the supply chain threat model be implemented to understand the potential threats and corresponding measurements?*", and we answered by introducing a SC threat analysis based on the CIST threat model. We showed that the CIST model with its four threat categories, i.e., counterfeiting, information leakage, sabotage, and tampering, can be applied in different SCs, e.g., electronic, food and

pharmaceutical. Together with the threats for each analyzed SC, we also provided the associated countermeasures.

We answered Q2 which is "*What are the security solutions for SC traceability and the limitations of current studies?"* by listing the current solutions and analysing the limitations of current tracking solutions.

Based on our analysis, several future research directions in this field can be listed as follow:

1. The provided security threat analyses in the existing SC solutions are limited to SC threats (e.g., overproduction, recycling, illegitimate device registration). The SC system is a vast network and can become more complex with the adoption of technologies like blockchain technology and IoT devices. Ensuring system security is extremely challenging, and the attacker can exploit unexpected vulnerabilities to damage the system and its interconnected suppliers. Although several solutions cover specific SC attacks for electronic goods, the research on food and pharmaceutical SCs that use electronic products in their solutions still require further security analysis. The SC network has an extensive connected structure where the potential risk in one organization can have a domino effect on the interconnected suppliers. Since a significant percentage of the existing works are built in a framework in which the suppliers are assumed as trusted. A single malicious SC entity can threaten an entire security system.
2. The current studies do not include the relationship with off-chain distribution among suppliers where the companies may purchase products from the suppliers that do not involve in the proposed tracking solution. Therefore, they might not be able to provide security to SC entities for the off-chain supplier. In this case, the existing solution can be limited to meet real-life SC systems' requirements.
3. Another interesting open challenge is the secondary market. The product sold through the secondary market opens a new way to sell and buy the excess inventory or refurbished products. However, the comprehensive security solution for the electronic product sold through the secondary market has not been considered. The secondary market is one of the critical parts of today's digital SC, which should be considered while introducing a secure system.

While this paper offers a broad perspective on SC security threats, it is subject to limitations that future studies should consider. Firstly, our analysis primarily focused on three types of supply chains: digital, food, and pharmaceutical. This focus potentially limits the generalizability of our findings as there are numerous other supply chains, such as software supply chains, which might present unique challenges and threats not covered in this study. Further SC threats can be identified for each SC type, and possible mitigation techniques against them can be introduced.

7 Conclusion

This paper analyses the security of the global SC in terms of security threats and existing traceability solutions. Our main key findings can be listed as follows:

- The SC system is a complex network. Implementing advanced technologies in SC security solutions can increase the network's complexity. Therefore, protecting the system against cyber

threats may become more challenging for organizations. Analysing the system's threats can provide a broad understanding to the developer to implement strong security against SC attacks. From this perspective, the security analysis of the existing solutions is limited in covering comprehensive SC threats.

- Blockchain and other technologies such as RFID, PUF, smart contracts used in the SC solutions may need to be investigated with actual data from SC organizations to prove the effectiveness of current solutions.

While this paper presents a broad perspective on SC security threats, this study is subjected to several limitations, which should be addressed in future studies. We analyzed different systems that implement advanced technologies to provide security and product quality, such as RFID for food quality, blockchain for data integrity, PUF for product authentication. Although this work illustrates the extended threat analysis, further SC threats can be identified for each SC type, and possible mitigation techniques against them can be introduced. Secondly, our analysis aim is specific to SC security threats; however, this can be extended with more technologies used in SC management, such as machine learning, cloud computing, and big data analytics. Lastly, interviews and case studies should be conducted with organizations to verify the effects of cyber threats on companies and investigate the protection efficiency of the proposed solutions on the organizations' operations.

References:

Abbas, K., Afaq, M., Khan, T.A. and Song, W.C. (2020), "A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry", *Electronics (Switzerland)*, Vol. 9 No. 5, pp. 1–31, doi: 10.3390/electronics9050852.

Ahmadi, V., Benjelloun, S., El Kik, M., Sharma, T., Chi, H. and Zhou, W. (2020), "Drug Governance: IoT-based Blockchain Implementation in the Pharmaceutical Supply Chain", *2020 6th International Conference on Mobile and Secure Services, MOBISECSERV 2020*, IEEE, pp. 1–8, doi: 10.1109/MobiSecServ48690.2020.9042950.

Ahmed, C.M., Gauthama Raman, M.R. and Mathur, A.P. (2020), "Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems", *CPSS 2020 - Proceedings of the 6th ACM Cyber-Physical System Security Workshop, Co-Located with AsiaCCS 2020*, pp. 23–29, doi: 10.1145/3384941.3409588.

Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M. and Wilczynski, A. (2020), "Anti-BlUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF", *International Journal of Information Security*, Springer Berlin Heidelberg, doi: 10.1007/s10207-020-00513-8.

Badia-Melis, R., Mishra, P. and Ruiz-García, L. (2015), "Food traceability: New trends and recent advances. A review", *Food Control*, Elsevier Ltd, Vol. 57, pp. 393–401, doi: 10.1016/j.foodcont.2015.05.005.

Bibi, F., Guillaume, C., Gontard, N. and Sorli, B. (2017), "A review: RFID technology having sensing aptitudes for food industry and their contribution to tracking and monitoring of food products", *Trends in Food Science and Technology*, Elsevier Ltd, Vol. 62, pp. 91–103, doi: 10.1016/j.tifs.2017.01.013.

Boyens, J., Paulsen, C., Bartol, N., Winkler, K. and Gimbi, J., 2021. *Key practices in cyber supply chain risk management: Observations from industry* (No. NIST Internal or Interagency Report (NISTIR) 8276). National Institute of Standards and Technology.

Bocek, T., Rodrigues, B.B., Strasser, T. and Stiller, B. (2017), "Blockchains everywhere - A use-case of blockchains in the pharma supply-chain", *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management*, pp. 772–777, doi: 10.23919/INM.2017.7987376.

Bumblauskas, D., Mann, A., Dugan, B. and Rittmer, J. (2020), "A blockchain use case in food distribution: Do you know where your food has been?", *International Journal of Information Management*, Elsevier, Vol. 52 No. September 2019, p. 102008, doi: 10.1016/j.ijinfomgt.2019.09.004.

Businessweek, B. (2018), "The Big Hack : How China Used a Tiny Chip to In fi ltrate U . S . Companies", pp. 1–13.

Cao, S., Powell, W., Foth, M., Natanelov, V., Miller, T. and Dulleck, U. (2021), "Strengthening consumer trust in beef supply chain traceability with a blockchain-based human-machine reconcile mechanism", *Computers and Electronics in Agriculture*, Elsevier B.V., Vol. 180 No. July 2020, p. 105886, doi: 10.1016/j.compag.2020.105886.

Caro, M.P., Ali, M.S., Vecchio, M. and Giaffreda, R. (2018), "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation", *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany, IOT Tuscany 2018*, IEEE, pp. 1–4, doi: 10.1109/IOT-TUSCANY.2018.8373021.

Casino, F., Kanakaris, V., Dasaklis, T.K., Moschuris, S., Stachtiaris, S., Pagoni, M. and Rachaniotis, N.P. (2020), "Blockchain-based food supply chain traceability: a case study in the dairy sector", *International Journal of Production Research*, Taylor & Francis, Vol. 0 No. 0, pp. 1–13, doi: 10.1080/00207543.2020.1789238.

Cheung, K.F., Bell, M.G.H. and Bhattacharjya, J. (2021), "Cybersecurity in logistics and supply chain management: An overview and future research directions", *Transportation Research Part E: Logistics and Transportation Review*, Elsevier Ltd, Vol. 146 No. December 2020, p. 102217, doi: 10.1016/j.tre.2020.102217.

Croom, S., Romano, P. and Giannakis, M., 2000. Supply chain management: an analytical framework for critical literature review. *European journal of purchasing & supply management*, *6*(1), pp.67-83.

Chien, W., De Jesus, J., Taylor, B., Dods, V., Alekseyev, L., Shoda, D. and Shieh, P.B. (2020), "The Last Mile: DSCSA Solution Through Blockchain Technology: Drug Tracking, Tracing, and Verification at the Last Mile of the Pharmaceutical Supply Chain with BRUINchain", *Blockchain in Healthcare Today*, doi: 10.30953/bhty.v3.134.

Cocco, L., Mannaro, K., Tonelli, R., Mariani, L., Lodi, M.B., Melis, A., Simone, M., *et al.* (2021), "A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery", *IEEE Access*, Vol. 9, pp. 62899–62915, doi: 10.1109/ACCESS.2021.3074874.

Colicchia, C., Creazza, A. and Menachof, D.A. (2019), "Managing cyber and information risks in supply chains: insights from an exploratory analysis", *Supply Chain Management*, Vol. 24 No. 2, pp. 215–240, doi: 10.1108/SCM-09-2017-0289.

Costa, C., Antonucci, F., Pallottino, F., Aguzzi, J., Sarriá, D. and Menesatti, P. (2013), "A Review on Agri-food Supply Chain Traceability by Means of RFID Technology", *Food and Bioprocess Technology*, Springer Science and Business Media, LLC, 1 February, doi: 10.1007/s11947-012-0958-7.

Cui, P., Dixon, J., Guin, U. and Dimase, D. (2019), "A Blockchain-Based Framework for Supply Chain Provenance", *IEEE Access*, IEEE, Vol. 7, pp. 157113–157125, doi: 10.1109/ACCESS.2019.2949951.

Dasaklis, T.K., Casino, F. and Patsakis, C. (2019), "A traceability and auditing framework for electronic equipment reverse logistics based on blockchain : the case of mobile phones", *ArXiv Preprint ArXiv:2005.11556*.

Ding, Q., Gao, S., Zhu, J. and Yuan, C. (2020), "Permissioned Blockchain-Based Double-Layer Framework for Product Traceability System", *IEEE Access*, IEEE, Vol. 8, pp. 6209–6225, doi: 10.1109/ACCESS.2019.2962274.

ENISA. (2021), *Enisa Landscape for Supply Chain Attacks*, doi: 10.2824/168593.

Garg, T., Kagalwalla, N., Churi, P., Pawar, A. and Deshmukh, S. (2020), "A survey on security and privacy issues in IoV", *International Journal of Electrical and Computer Engineering*, Vol. 10 No. 5, pp. 5409–5419, doi: 10.11591/IJECE.V10I5.PP5409-5419.

Grecuccio, J., Giusto, E., Fiori, F. and Rebaudengo, M. (2020), "Combining blockchain and iot: Food-chain traceability and beyond", *Energies*, Vol. 13 No. 15, doi: 10.3390/en13153820.

Grobauer, B., Walloschek, T. and Stöcker, E. (2011), "Understanding cloud computing vulnerabilities", *IEEE Security and Privacy*, Vol. 9 No. 2, pp. 50–57, doi: 10.1109/MSP.2010.115.

Guin, U., Cui, P. and Skjellum, A. (2018), "Ensuring Proof-of-Authenticity of IoT Edge Devices Using Blockchain Technology", *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, IThings/Gree*, pp. 1042–1049, doi: 10.1109/Cybermatics_2018.2018.00193.

Guin, U., Dimase, D. and Tehranipoor, M. (2014), "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead", *Journal of Electronic Testing: Theory and Applications (JETTA)*, Vol. 30 No. 1, pp. 9–23, doi: 10.1007/s10836-013-5430-8.

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

Halak, B. (2021), "CIST: A Threat Modelling Approach for Hardware Supply Chain Security", *Hardware Supply Chain Security*, pp. 3–65, doi: 10.1007/978-3-030-62707-2_1.

Hassija, V., Chamola, V., Gupta, V., Jain, S. and Guizani, N. (2020), "A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures", *IEEE Internet of Things Journal*, Vol. 333031 No. c, pp. 1–1, doi: 10.1109/jiot.2020.3025775.

Hayati, H. and Gusti Bagus Baskara Nugraha, I. (2018), "Blockchain based traceability system in food supply chain", *2018 International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2018*, IEEE, pp. 120–125, doi: 10.1109/ISRITI.2018.8864477.

Islam, M.N., Patii, V.C. and Kundu, S. (2018), "On IC traceability via blockchain", *2018 International Symposium on VLSI Design, Automation and Test, VLSI-DAT 2018*, pp. 1–4, doi: 10.1109/VLSI-DAT.2018.8373269.

James, E.R. (2021), "Disrupting vaccine logistics", *International Health*, Vol. 13 No. 3, pp. 211–214, doi: 10.1093/inthealth/ihab010.

Kamath, R. (2018), "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM", *The Journal of the British Blockchain Association*, Vol. 1 No. 1, pp. 1–12, doi: 10.31585/jbba-1-1-(10)2018.

Khan, P.W., Byun, Y.C. and Park, N. (2020), "IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning", *Sensors (Switzerland)*, Vol. 20 No. 10, pp. 1–24, doi: 10.3390/s20102990.

Kieras, T., Farooq, J. and Zhu, Q. (2021), "I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions", *IEEE Access*, Vol. 9, pp. 29827–29840, doi: 10.1109/ACCESS.2021.3058338.

Kieras, T., Farooq, M.J. and Zhu, Q. (2020), "RIoTS: Risk Analysis of IoT Supply Chain Threats", *IEEE World Forum on Internet of Things, WF-IoT 2020 - Symposium Proceedings*, pp. 1–6, doi: 10.1109/WF-IoT48130.2020.9221323.

Kim, M., Hilton, B., Burks, Z. and Reyes, J. (2018), "IoT to Design a Food Traceability Solution", *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, IEEE, No. Figure 1, pp. 335–340.

Kim, M., Hilton, B., Burks, Z. and Reyes, J. (2019), "Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution", *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018*, doi: 10.1109/IEMCON.2018.8615007.

Kulkarni, A., Hazari, N.A. and Niamat, M. (2019), "A Blockchain Technology Approach for the Security and Trust of the IC Supply Chain", *Proceedings of the IEEE National Aerospace Electronics Conference, NAECON*, IEEE, Vol. 2019-July, pp. 249–252, doi: 10.1109/NAECON46414.2019.9058027.

Kumar, R. and Tripathi, R. (2019a), "Traceability of counterfeit medicine supply chain through Blockchain", *2019 11th International Conference on Communication Systems and Networks, COMSNETS 2019*, IEEE, Vol. 2061 No. 1, pp. 568–570, doi: 10.1109/COMSNETS.2019.8711418.

Kumar, R. and Tripathi, R. (2019b), "Traceability of counterfeit medicine supply chain through Blockchain", *2019 11th International Conference on Communication Systems and Networks, COMSNETS 2019*, IEEE, Vol. 2061 No. 1, pp. 568–570, doi: 10.1109/COMSNETS.2019.8711418.

Leung, H.W. and Chapman, A. (2020), "Identifying Food Fraud Using Blockchain".

Lin, J., Zhang, A., Shen, Z. and Chai, Y. (2018), “Blockchain and IoT based food traceability for smart agriculture”, *ACM International Conference Proceeding Series*, pp. 1–6, doi: 10.1145/3126973.3126980.

Litke, A., Anagnostopoulos, D. and Varvarigou, T. (2019), “Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment”, *Logistics*, Vol. 3 No. 1, p. 5, doi: 10.3390/logistics3010005.

Liu, X., Barenji, A.V., Li, Z., Montreuil, B. and Huang, G.Q. (2021), “Blockchain-based smart tracking and tracing platform for drug supply chain”, *Computers and Industrial Engineering*, Elsevier Ltd, Vol. 161 No. July, p. 107669, doi: 10.1016/j.cie.2021.107669.

Mäde, D., Trübner, K., Neubert, E., Höhne, M. and Johne, R. (2013), “Detection and Typing of Norovirus from Frozen Strawberries Involved in a Large-Scale Gastroenteritis Outbreak in Germany”, *Food and Environmental Virology*, Vol. 5 No. 3, pp. 162–168, doi: 10.1007/s12560-013-9118-0.

Mehta, D., Lu, H., Paradis, O.P., M. S., M.A., Rahman, M.T., Iskander, Y., Chawla, P., *et al.* (2020), “The Big Hack Explained”, *ACM Journal on Emerging Technologies in Computing Systems*, Vol. 16 No. 4, pp. 1–25, doi: 10.1145/3401980.

Mondal, S., Wijewardena, K.P., Karuppuswami, S., Kriti, N., Kumar, D. and Chahal, P. (2019), “Blockchain inspired RFID-based information architecture for food supply chain”, *IEEE Internet of Things Journal*, Vol. 6 No. 3, pp. 5803–5813, doi: 10.1109/JIOT.2019.2907658.

Moysiadis, T., Spanaki, K., Kassahun, A., Kläser, S., Becker, N., Alexiou, G., Zotos, N. and Karali, I., 2022. AgriFood supply chain traceability: Data sharing in a farm-to-fork case. *Benchmarking: An International Journal*.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Al-hammadi, M.D.Y. and Ellaham, S. (2021), “A Blockchain-based Approach for Drug Traceability in Healthcare Supply Chain”, doi: 10.1109/ACCESS.2021.3049920.

Naeem Firdous, S., Traceability in supply chains: A Cyber security analysis. *Computers & Security*.

Nazmul Islam, M.D. and Kundu, S. (2019), “Enabling IC traceability via blockchain pegged to embedded PUF”, *ACM Transactions on Design Automation of Electronic Systems*, Vol. 24 No. 3, doi: 10.1145/3315669.

Negka, L., Gketsios, G., Anagnostopoulos, N.A., Spathoulas, G., Kakarountas, A. and Katzenbeisser, S. (2019), “Employing blockchain and physical unclonable functions for counterfeit IoT devices detection”, *ACM International Conference Proceeding Series*, Vol. Part F1481, pp. 172–178, doi: 10.1145/3312614.3312650.

Patil, A.S., Tama, B.A., Park, Y. and Rhee, K.H. (2018), “A framework for blockchain based secure smart green house farming”, *Lecture Notes in Electrical Engineering*, Vol. 474, pp. 1162–1167, doi: 10.1007/978-981-10-7605-3_185.

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., *et al.* (2021), “Perspectives on the SolarWinds Incident”, *IEEE Security and Privacy*, Vol. 19 No. 2, pp. 7–13, doi: 10.1109/MSEC.2021.3051235.

Polypufs, M.A., Fsms, P.U.F. and Notation, A. (2019), “Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF–FSMs”, IEEE, Vol. 14 No. 8, pp. 2043–2058.

Raj, R., Rai, N. and Agarwal, S. (2019), “Anticounterfeiting in Pharmaceutical Supply Chain by establishing Proof of Ownership”, *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, IEEE, Vol. 2019-Octob, pp. 1572–1577, doi: 10.1109/TENCON.2019.8929271.

Ram, K. and Pant, D. (2010), "A threat risk modeling framework for Geospatial Weather Information System (GWIS) a DREAD based study", *International Journal of Advanced Computer Science and Applications*, Vol. 1 No. 3, pp. 20–28, doi: 10.14569/ijacsa.2010.010304.

Saitta, P., Larcom, B. and Eddington, M. (2005), "Trike v. 1 methodology document", *URL: Http://Dymaxion. Org/Trike/ ...*, pp. 1–17.

Salah, K., Nizamuddin, N., Jayaraman, R. and Omar, M. (2019), "Blockchain-Based Soybean Traceability in Agricultural Supply Chain", *IEEE Access*, IEEE, Vol. 7, pp. 73295–73305, doi: 10.1109/ACCESS.2019.2918000.

Spanaki, K., Karafili, E. and Despoudi, S., 2022. Digital architectures: frameworks for supply chain data and information governance. In *The Digital Supply Chain* (pp. 147-161). Elsevier.

Sancho, J.C., Caro, A., Ávila, M. and Bravo, A. (2020), "New approach for threat classification and security risk estimations based on security event management", *Future Generation Computer Systems*, Elsevier B.V., Vol. 113, pp. 488–505, doi: 10.1016/j.future.2020.07.015.

Simopoulos, D., Avino, L.D. and Wolf, A. (2021), "The PASTA threat model implementation in the IoT development life cycle".

Sinclair, D., Shahriar, H. and Zhang, C. (2019), "Security requirement prototyping with hyperledger composer for drug supply chain – A blockchain application", *ACM International Conference Proceeding Series*, pp. 158–163, doi: 10.1145/3309074.3309104.

Storey, J., Emberson, C., Godsell, J. and Harrison, A., 2006. Supply chain management: theory, practice and future challenges. *International Journal of Operations & Production Management*, *26*(7), pp.754-774.

Sunny, J., Undralla, N. and Madhusudanan Pillai, V. (2020), "Supply chain transparency through blockchain-based traceability: An overview with demonstration", *Computers and Industrial Engineering*, Elsevier Ltd, Vol. 150 No. October, p. 106895, doi: 10.1016/j.cie.2020.106895.

Syed, N.F., Shah, S.W., Trujillo-Rasua, R. and Doss, R. (2022), "Traceability in supply chains: A Cyber security analysis", *Computers and Security*, Elsevier Ltd, Vol. 112, p. 102536, doi: 10.1016/j.cose.2021.102536.

Sylim, P., Liu, F., Marcelo, A. and Fontelo, P. (2018), "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention", *Journal of Medical Internet Research*, Vol. 20 No. 9, pp. 1–12, doi: 10.2196/10163.

Tian, F. (2016), "An agri-food supply chain traceability system for China based on RFID & blockchain technology", *2016 13th International Conference on Service Systems and Service Management, ICSSSM 2016*, IEEE, doi: 10.1109/ICSSSM.2016.7538424.

Tian, F. (2017a), "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things", *14th International Conference on Services Systems and Services Management, ICSSSM 2017 - Proceedings*, IEEE, doi: 10.1109/ICSSSM.2017.7996119.

Tian, F. (2017b), "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things", *14th International Conference on Services Systems and Services Management, ICSSSM 2017 - Proceedings*, IEEE, doi: 10.1109/ICSSSM.2017.7996119.

Tieyan, L. and Robert, D. (2007), "Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol", *Proceedings - Second International Conference on*

Availability, Reliability and Security, ARES 2007, pp. 238–245, doi: 10.1109/ARES.2007.159.

Tseng, J.H., Liao, Y.C., Chong, B. and Liao, S.W. (2018), "Governance on the drug supply chain via gcoin blockchain", *International Journal of Environmental Research and Public Health*, Vol. 15 No. 6, doi: 10.3390/ijerph15061055.

Valenza, F., Karafili, E., Steiner, R.V. and Lupu, E.C., 2022. A hybrid threat model for smart systems. *IEEE Transactions on Dependable and Secure Computing*.

Wang, S., Li, D., Zhang, Y. and Chen, J. (2019), "Smart Contract-Based Product Traceability System in the Supply Chain Scenario", *IEEE Access*, IEEE, Vol. 7, pp. 115122–115133, doi: 10.1109/access.2019.2935873.

Wu, X. and Lin, Y. (2019), "Blockchain recall management in pharmaceutical industry", *Procedia CIRP*, Elsevier B.V., Vol. 83, pp. 590–595, doi: 10.1016/j.procir.2019.04.094.

Xiao, Q., Gibbons, T. and Lebru, H. (2009), "RFID Technology, Security Vulnerabilities, and Countermeasures", *Supply Chain the Way to Flat Organisation*, No. January, doi: 10.5772/6668.

Xu, X., Rahman, F., Shakya, B., Vassilev, A., Forte, D. and Tehranipoor, M. (2019), "Electronics Supply Chain Integrity Enabled by Blockchain", Vol. 24 No. 3.

Yang, K., Forte, D. and Tehranipoor, M. (2015), "An RFID-based technology for electronic component and system Counterfeit detection and Traceability", *2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015*, IEEE, No. 3, doi: 10.1109/THS.2015.7225279.

Yang, K., Forte, D. and Tehranipoor, M.M. (2017), "Cdta", *ACM Transactions on Design Automation of Electronic Systems*, Vol. 22 No. 3, pp. 1–31, doi: 10.1145/3005346.

Zhang, Y. and Guin, U. (2020), "End-to-End Traceability of ICs in Component Supply Chain for Fighting against Recycling", *IEEE Transactions on Information Forensics and Security*, IEEE, Vol. 15, pp. 767–775, doi: 10.1109/TIFS.2019.2928493.

Appendix

Solution	Year	Supply Chain Type	Security Objective	Addressed Challenged	Technology	Advantages	Limitation	Target in Supply Chain
IC traceability (Islam *et al.*, 2018)	2018	Electronic	Anti-counterfeits	Visibility Traceability Untrusted third-party vendors	Blockchain Smart contract PUF Chaincode	Tamper-proof solution to track ICs against counterfeited products.	No detail on PUF data management and smart contracts implementation.	Traceability
Tracking of IC supply chain (Cui *et al.*, 2019)	2019	Electronic	Anti-counterfeits	Traceability Untrusted third-party vendors	Blockchain Smart contract PUF Chaincode	The system feasibility is shown.	No tracking solution for the independent distributors.	Traceability
Authentication of IoT edge devices (Guin *et al.*, 2018)	2018	Electronic	Anti-counterfeits Proof-of-Authenticity	Traceability Untrusted third-party vendors	Blockchain SRAM PUF Smart contract Key-value store	Periodic authentication mechanisms to protect against rogue device entrance.	No implementation cost information.	Authentication for IoT devices in SC
Counterfeit IoT devices detection (Negka *et al.*, 2019)	2019	Electronic	Tamper-proof Anti-counterfeits	Traceability	Blockchain Smart contract PUF	PUF for the used IoTs to mitigate the counterfeits and cloned devices.	No details on IoTs attacks prevention.	Traceability
IC traceability (Nazmul Islam and Kundu, 2019)	2019	Electronic	Resistance against cloning	Visibility Traceability Untrusted third-party vendors	Blockchain Smart contract PUF	Software application for ICs verification.	Vulnerabilities in the authentication system not considered.	Traceability
IC supply chain integrity (Xu *et al.*, 2019)	2018	Electronic	Resistance against cloning, recycling, overproducti	Traceability Untrusted third-party vendors	Blockchain Smart contract PUF	Solution against common security	No implementation cost information.	Integrity

			on, remarking			vulnerabilities.		
Counterfeit mitigation in IC supply chain (Aniello *et al.*, 2020)	2020	Electronic	Anti-counterfeits	Visibility Traceability Untrusted third-party vendors Accountability	Blockchain Smart contract PUF	Traceability solution and threat model.	Do not cover SC risks like off-chain distribution.	Anti-counterfeit
Product Traceability (Ding *et al.*, 2020)	2020	Electronic	Anti-counterfeits	Traceability	Blockchain Smart contract	Improved scalability and performance.	Higher costs due to multi-blockchain use.	Traceability
Agri-food supply chain traceability (Tian, 2016)	2016	Food	Anti-counterfeits	Traceability	Blockchain RFID	Track and trace solutions. SC information identification.	No details on attack prevention and vulnerabilities mitigation.	Traceability
Traceability for food safety (Tian, 2017a)	2017	Food	Anti-counterfeits	Visibility Traceability Untrusted third-party vendors	Blockchain Smart contract HACCP IoTs	Provides the SC processes details.	No implementation details.	Traceability for food safety.
Traceability for food supply chain (Caro *et al.*, 2018)	2018	Food	Resistance against cloning Anti-counterfeits Proof-of-Authenticity	Traceability Untrusted third-party vendors	Blockchain Smart contract IoTs	Edge devices are use as full nodes of the blockchain. Enhanced networks robustness.	High transaction costs and no implementation details.	Agri-food SC traceability.
Traceability for food supply chain (Casino *et al.*, 2020)	2020	Food	Anti-cloning	Visibility Traceability	Blockchain Smart contract	Smart contract technologies to improve products' safety and quality.	No details on IoT devices protection.	Tracing for dairy-food SC.
Pharmaceutical supply chain's integrity (Bocek *et al.*, 2017)	2017	Pharmaceutical	Data integrity	Traceability	Blockchain Smart contract IoTs Electronic sensors	Maintain good quality in pharmaceutical SC.	High transaction costs and no security analysis.	Data immutability

Traceability of medicine supply chain (Kumar and Tripathi, 2019a)	2019	Pharmaceutical	Anti-counterfeits	Traceability	Blockchain Encrypted QR code	Drug authenticity.	No security analysis and no implementation details.	Anti-counterfeiting

Table 5 Summary of the Traceability Solutions in SC