A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures

Vikas Hassija, Vinay Chamola, *Senior Member, IEEE*, Vatsal Gupta, Sarthak Jain, and Nadra Guizani

***Abstract*—The rapid improvement in the global connectivity standards has escalated the level of trade taking place among different parties. Advanced communication standards are allowing the trade of all types of commodities and services. Furthermore, the goods and services developed in a particular region are transcending boundaries to enter into foreign markets. Supply chains play an essential role in the trade of these goods. To be able to realize a connected world with no boundary restrictions in terms of goods and services, it is imperative to keep the associated supply chains transparent, secure, and trustworthy. Therefore, some fundamental changes in the current supply chain architecture are essential to achieve a secure trade environment. This article discusses the supply chain's security-critical application areas and presents a detailed survey of the security issues in the existing supply chain architecture. Various emerging technologies, such as blockchain, machine learning (ML), and physically unclonable functions (PUFs) as solutions to the vulnerabilities in the existing infrastructure of the supply chain have also been discussed. Recent studies reviewed in this work reveal a growing sentiment in the industry toward new and emerging technologies, such as Internet of Things (IoT), blockchain, and ML. While many organizations have already adopted IoT applications and artificial intelligence systems in their businesses, widespread adoption of blockchain remains distant. It has also been found that over the past decade, PUF-based authentication systems have gained much ground. However, a proper reference model for their implementation in complex supply chains is still missing.**

***Index Terms*—Artificial intelligence (AI), blockchain, cloud computing, counterfeit, cybersecurity, machine learning (ML), physically unclonable functions (PUFs), supply chain, supply chain security.**

I. Introduction

THE DEFINITION of a supply chain goes well beyond the flow of materials alone. It includes the flow of information, services, and finances. Even if one considers a single factory at a single-location operating with just a few suppliers, the supply chain process is a complicated operation that requires effective communication and a supportive organizational culture. The supply chain forms the backbone of the current consumer-first world. Every commodity in the market moves through a sequence of stakeholders who engage in a sophisticated manner to deliver the final product. Modern-day supply chains span across multiple geographical boundaries in different socioeconomic dimensions, each requiring its specific set of checks and balances to ensure smooth functioning of the chain. Furthermore, with the introduction of technologies, such as the Internet of Things (IoT) and 5G, the efficacy and utility of supply chain management have improved significantly.

The supply chain is necessary for almost all domains, including the pharmaceutical industry, the agricultural products industry, the gem industry, and the electrical appliance industry. It is, therefore, essential to keep the supply chain functioning uninterruptedly through various security checks. However, the exponentially growing variables in the existing system have made this process highly complicated. Owing to certain inefficiencies in the current supply chain ecosystem, the quality of products often gets substantially degraded before reaching the end users. Additionally, the prevailing shortcomings in supply chain security have augmented the issue of counterfeit and pirated goods. This leads to a monetary loss for the consumers as well as a loss of reputation for the manufacturers. The complicated nature of the supply chain makes it challenging to track and retrace every step in the chain. Several perpetrators take advantage of this vulnerability and engage in different kinds of malicious activities like piracy for their financial benefits.

A. Motivation

Trade of counterfeit and pirated products has gradually increased in the past few years, presenting a major challenge to the innovation-driven global economy. Despite the stagnant overall trade volumes, the trade of counterfeit/pirated products has surged from 2.5% of the worldwide trade in 2013 to 3.3% in 2016, as per a report published by the Organization for Economic Co-operation and Development (OECD) and the European Union (EU) in 2019 [1]. During the same period, the global value of counterfeit goods has also increased from $461 billion to $509 billion. For the EU, the import of counterfeit goods with respect to the total imports from non-EU nations increased from 5% in 2013 to 6.8% in 2016. United States (24%), France (17%), Italy (15%), Switzerland (11%), and Germany (9%) (as % of total trade in the country) were few of the most affected countries due to counterfeiting in 2016.

Manuscript received July 20, 2020; revised September 18, 2020; accepted September 18, 2020. Date of publication September 22, 2020; date of current version April 7, 2021. *(Corresponding author: Vinay Chamola.)*

Vikas Hassija, Vatsal Gupta, and Sarthak Jain are with the Department of Computer Science and IT, Jaypee Institute of Information Technology, Noida 201304, India (e-mail: vikas.hassija@jiit.ac.in; vatsalgupt99@gmail.com; sarthakjain505@gmail.com).

Vinay Chamola is with the Department of Electrical and Electronics Engineering and also with the APPCAIR, Birla Institute of Technology and Science Pilani, Pilani 333031, India (e-mail: vinay.chamola@pilani.bits-pilani.ac.in).

Nadra Guizani is with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164 USA (e-mail: nguizani@purdue.edu).

Digital Object Identifier 10.1109/JIOT.2020.3025775

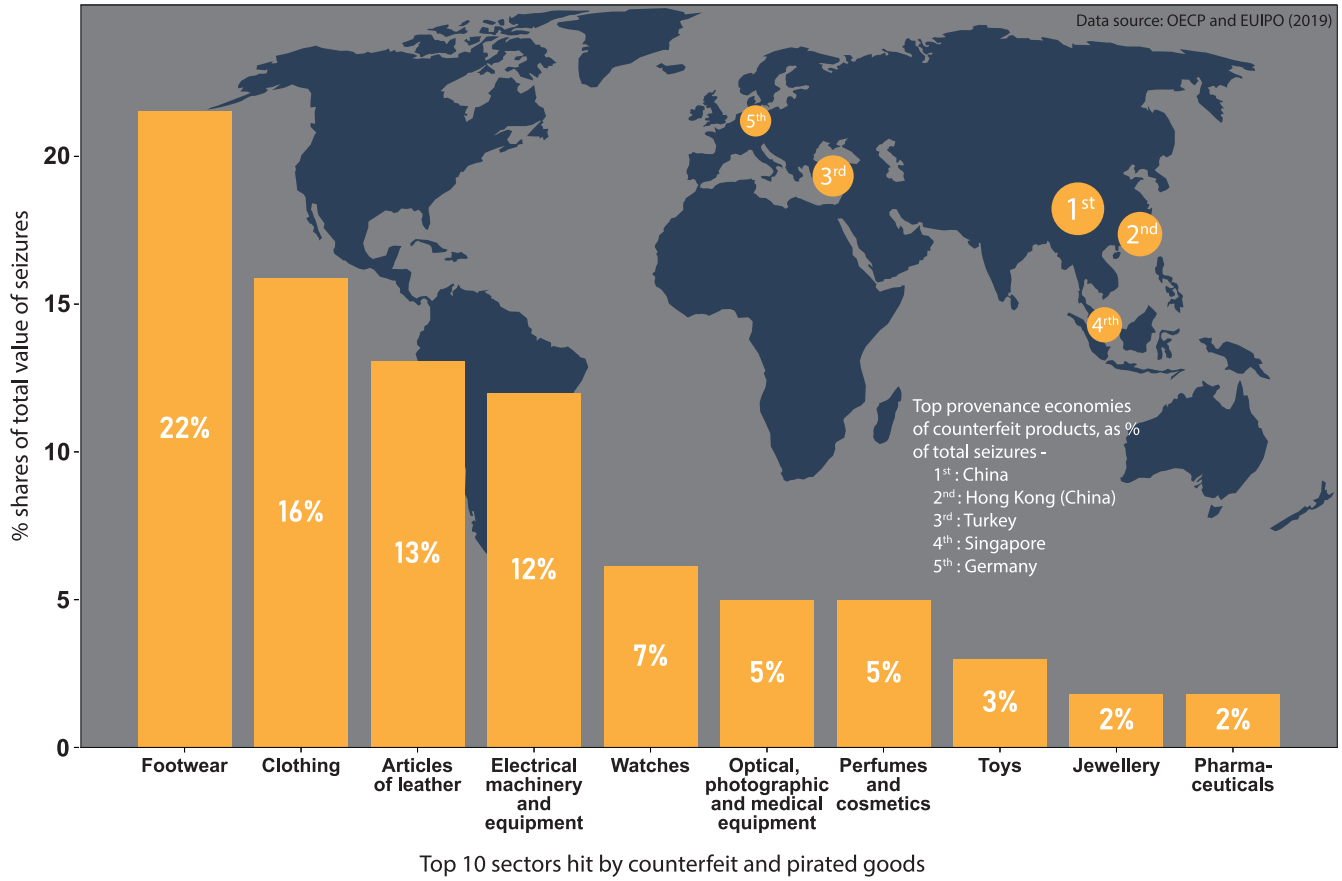

Fig. 1. Outlook on the type and source of counterfeit goods (Data source: OECP and EUIPO—2019).

An increasing number of industries in Hong Kong, Singapore, and other emerging economies like Brazil, China, and India are also becoming prone to counterfeiting (refer to Fig. 1) [1].

Besides counterfeiting and other types of physical threats that have been major concerns for the supply chain managers for decades, managers of modern supply chains also encounter an increasing number of challenges associated with information security. The increase in such challenges is attributed to the evolution of the Internet infrastructure, to the point where well operated, effective supply chains rely on a variety of interdependent software and hardware; that collect and transmit critical data on shipments, inventory, and equipment state, among other aspects. This heavy reliance on technology provides malicious parties with new ways to disrupt supply chains and obtain confidential data or, in some cases, money [2].

Over the past decade, various attempts have been made in both industry and academia to enhance the level of transparency and security in the supply chains. To minimize manual intervention and reduce the risk of corruption, most of the paperwork today is being digitized, while various other processes are being automated through the use of diverse technologies. Although such attempts have made a significant contribution to this field, a more robust security framework is required to secure the end-to-end flow of products in the supply chain for an exponentially growing market [3]. To this end, it is essential to incorporate the latest technological advances. In this survey, we provide a comprehensive review of the security issues in the current supply chain architecture and the improvements required to overcome them. Furthermore, the use of various technologies, including blockchain, machine learning (ML), and physically unclonable functions (PUFs), has been examined as a means to secure the supply chain processes.

B. Organization

The remainder of the work is organized as follows. Section II discusses the literature in the domain of supply chain security and highlights our contribution to the same. Section III addresses different sources of threats and existing security challenges at different levels of the supply chain. Section IV addresses the security-critical application areas of the supply chain, while Section V lays down the improvements required in the traditional supply chain architecture to establish a more secure and efficient supply chain. Sections VI–IX review the three leading solutions to supply chain security, namely, blockchain, ML, and PUFs. Section X discusses the issues, challenges, and the future scope of research in the direction of supply chain security, while Section XI concludes this article. All the acronyms used in this article are listed in Table I.

C. Our Contributions

The main contributions of this work are enumerated as follows.

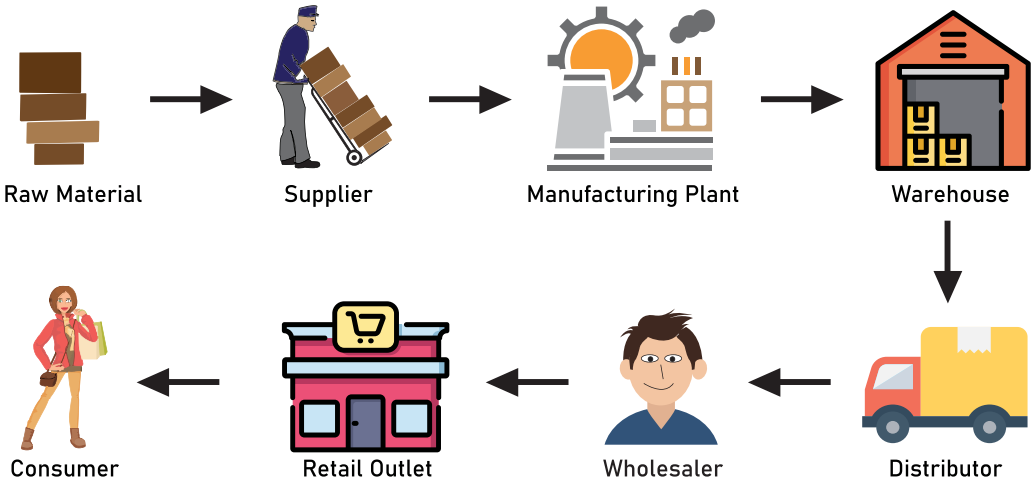

Fig. 2. Traditional supply chain.

TABLE I
LIST OF ACRONYMS

Notation	Meaning
PUF	Physical Unclonable Functions
UAVs	Unmanned Aerial Vehicles
OECD	Organization for Economic Co-operation and Development
DMFBs	Digital Microfluidic Biochips
RFID	Radio Frequency Identification
SCoT	Supply Chain of Things
ASC	Agri-Food Products Supply Chain
EIA	Energy Information Administration
OPEC	Organization of the Petroleum Exporting Countries
DLT	Distributed Ledger Technology
API	Application Programming Interface
PoC	Proof of Concept
IDG	International Data Group
RPA	Robotic Process Automation
NLP	Natural Language Processing
SVM	Support Vector Machines
ACID	Anomalous Container Itinerary Detection
CSM	Container System Messages
GPRS	General Packet Radio Service
GIS	Geographic Information System
SSD	Solid State Drive
CRD	Challenge-Response Data
SRAM	Static Random Access Memory
CRP	Challenge-Response Pairs
IC	Integrated Circuit
DOS	Denial of Service

1) The security threats faced by a majority of traditional supply chains have been thoroughly reviewed, with the flow of a traditional supply chain given in Fig. 2.
2) Security and privacy issues associated with diverse areas of supply chain management have been categorized for the reader's ease of understanding.
3) Detailed recommendations have been provided for improving the supply chain infrastructure and facilitating secure communication among different participants of the supply chain.
4) Three technologies—blockchain, ML, and PUFs, have been identified as a means to resolve the security risks and other issues prevalent in traditional supply chains.
5) The future scope of research for developing secure supply chain applications has also been discussed for the benefit of future researchers.

II. Related Works

Supply chain security has become a subject of massive interest in both academia and industry. Several recent studies discuss the importance of security in supply chains and the measures required to achieve that. Lu *et al.* [4] have classified the supply chain security practices into four categories: mitigation, prevention, response, and detection. The authors have relied upon multiple indicators to operationalize each practice. Responses from 462 firms operating in Italy and the United States were also assessed to measure the relative efficiency of each practice. Al Sabbagh and Kowalski [5] presented a threat-modeling framework specific to the software supply chain. The authors identified countermeasure identification, threat modeling, and target system identification as the three main issues in the software supply chain.

Ali *et al.* [6] specifically discussed the security in the digital microfluidic biochips (DMFBs) supply chains. The study's primary objective was to examine ways to prevent attackers from exploiting the supply chain vulnerabilities and pirating DMFBs' proprietary protocols. Such exploitation could have severe implications for biotechnology innovation, healthcare, and laboratory analysis. Ralston *et al.* [7] explored the use of microscopic dielets embedded in the electronic components to address the issue of counterfeit electronic devices. According to the authors, the components' movements can be monitored via dielets [near-field radio-frequency identification (RFID) chips] embedded in the packaging of the electronic components.

Huang *et al.* [8] proposed a double-track approach to clone detection for RFID-enabled supply chains. They utilized the difference in the verification sequences of the RFID tags to distinguish the cloned tags from the genuine ones. Skudlarek *et al.* [9] examined the existing security concerns in the trade of electronic devices arising due to the fragmentation

of the system-on-chip supply chain. This study puts forth the use of unique chip IDs as a solution that allows all the stakeholders in the supply chain to authenticate, track, provision, and analyze all the products during the entire life cycle of the chip. Zhang *et al.* [10] and Wang *et al.* [11] have proposed a wrapper that is dynamically obfuscated on the chip to protect the supply chains against various types of piracy attacks.

Esfahani *et al.* [12] have presented a security mechanism based on Web authentication to prevent man-in-the-middle attacks in industry 4.0 Supply Chain. A transport layer security (TLS) protocol has been adopted for secure Internet communications between a user's Web browser and a remote server. Wu *et al.* [13] have put forth the concept of "Supply Chain of Things (SCoT)" to connect different layers and entities involved in the supply chain, as is done in the IoT. The model proposed in this work is expected to have a considerable impact on smart transportation, efficient integration, end-to-end traceability, and intelligent decision making.

In recent years, blockchain has been identified as a groundbreaking technology for use in various domains, such as industry 4.0 [14], unmanned aerial vehicles (UAVs) [15], vehicle-to-grid networks [16], intelligent transportation systems [17]–[20], mobile *ad hoc* networks [21], energy management [22], smart grids [23], and cellular network management [24], [25], to name a few. It is also being viewed as a solution to most of the security issues associated with supply chains. Various works, such as [26]–[28] focus on the use of blockchain to secure the supply chain and to track the movements of the items in an immutable distributed ledger. Table II has been compiled to list major works on the subject matter, i.e., the safety and security of the supply chain.

Despite the abundance of research on supply chain security, a detailed survey on all the existing and upcoming challenges in the supply chain application is much needed. This article is written to help the user in obtaining a well-reasoned design for cutting-edge methods available for supply chain security.

III. Security Vulnerabilities in Modern Supply Chains

Owing to the participation of several individuals, organizations, lawmakers, and potentially even nations, supply chain networks are overly complicated. Supply chains face various issues in terms of 1) generating trust among the various parties involved; 2) cyberattacks; 3) cargo theft; and 4) counterfeiting and many more [29]. Among stolen goods, food and beverages are the most common items; however, pharmaceuticals and electronics are the most expensive. The level of security threats that a supply chain faces is directly proportional to the complexity of that particular supply chain [30], i.e., an increase in the complexity of the supply chain increases the susceptibility of the supply chain to various kinds of security threats. These threats can affect vulnerabilities in many areas of supply chain operations [31].

1) Tampering and fraudulent substitution of goods can reduce their utility and render them unsatisfactory for the end user.
2) All the entities in the supply chain, especially the third-party service providers, might not have the same security standards.
3) In today's scenario, information technology (IT) systems drive large parts of the supply chain; therefore, cybersecurity is one of the most critical issues. Heavy dependence on an interconnected IT system exposes the chain to the single point of failure issue. Access to just one of the systems can lead to access to other secure parts.

A. Counterfeiting

As discussed in Section I-A, counterfeiting has proved to be one of the biggest concerns for all supply chain managers across the world. Counterfeiting not only impacts the sales and profits of the affected businesses but it is also detrimental to the economy as a whole. The broader implications of piracy include an adverse impact on public health, safety, and security [32]. In recent times, an increasing number of industries have fallen prey to counterfeiting. Counterfeit products are particularly common among consumer goods, such as footwear, toys, perfumes, cosmetics, phones, watches, and batteries (refer to Fig. 1). According to Forbes, counterfeiting was the most significant criminal enterprise in 2018 [33]. Among other risks, counterfeiting of goods like food products, beverages, pharmaceuticals, and medical equipment, can pose serious health and safety risks. The only way to limit piracy is to maintain control over the entire global supply chain and enforce discipline in the verification and monitoring of all the supply chain partners and products [34].

B. Cybersecurity Threats

Security issues can arise in all phases of a specific supply chain. The security measure of the overall supply chain can be characterized by its weakest link. A determined assailant will target this weakest link to gain unauthorized access to not only that link but also the other parts of the chain. Therefore, a high level of security is required in all parts of the supply chain, be it software or hardware, especially since it is not possible to predict the directions of the risk [35]. However, since the software component of the chain is more vulnerable to attacks from a remote location, special care is needed to ensure its security.

Cybersecurity, with respect to supply chain security, refers to the act of securing that part of the chain that deals with IT systems, networks, and software. Cybersecurity is essential to prevent confidential data from being stolen, and to ensure that any type of malware, spyware does not harm the system and, by extension, the entire chain [35]. Supply chains can face various kinds of cybersecurity threats; however, they are primarily centered around three main areas.

1) *Intellectual Property:* Many supply chains rely on keeping knowledge about their products within the chain itself. A deliberate leak of confidential information can threaten the viability of businesses throughout the chain.
2) *Sensitive Data:* To ensure the proper functioning of the supply chains, a systematic system that facilitates data-sharing among each link in the chain is required.

TABLE II
LITERATURE IN THE DIRECTION OF SUPPLY CHAIN SECURITY

Year	Author	Research Topic
2015	J. Huang *et al.*	DTD: A Novel Double-Track Approach to Clone Detection for RFID-Enabled Supply Chains
2016	P. Ralston *et al.*	Defeating counterfeiters with microscopic dielets embedded in electronic components
2016	J. P. Skudlarek *et al.*	A Platform Solution for Secure Supply-Chain and Chip Life-Cycle Management
2017	G. Lu *et al.*	A Classification of Practices and an Empirical Study of Differential Effects and Complementarity
2017	B. Al Sabbagh *et al.*	A Socio-technical Framework for Threat Modeling a Software Supply Chain
2017	S. S. Ali *et al.*	Supply-Chain Security of Digital Microfluidic Biochips
2017	X. Wang *et al.*	Secure Scan and Test Using Obfuscation Throughout Supply Chain
2018	D. Zhang *et al.*	An On-Chip Dynamically Obfuscated Wrapper for Protecting Supply Chain Against IP and IC Piracies
2019	K. Salah *et al.*	Blockchain-Based Soybean Traceability in Agricultural Supply Chain
2019	N. Kshetri *et al.*	Blockchain Adoption in Supply Chain Networks in Asia
2019	Q. Lin *et al.*	Food Safety Traceability System Based on Blockchain and EPCIS
2019	A. Esfahani *et al.*	An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Supply Chain
2019	C.K. Wu *et al.*	Supply Chain of Things: A Connected Solution to Enhance Supply Chain Productivity

However, such systems should ensure that the sensitive data being shared, such as consumer's credit card details, is not exposed.

3) *Cloud Technology:* Cloud-based data sharing has made data-sharing more rapid and prolific. However, sharing of data using cloud technology compromises the supply chain's privacy and makes it vulnerable to several types of malicious attacks [36].

C. Third Party Vendor Security Risks

Almost all the organizations around the globe depend on one or more third-party vendors to successfully actualize their business strategies. In most cases, such parties have access to the company's private data, internal information, and technology systems. However, these parties are not subject to the supply chain's internal risk management process, which generates a cyber risk for unauthorized intrusions. Furthermore, third-party vendors often have inadequate cyber protection techniques against illegal access, which is the primary reason for third party data breaches. In a survey carried out by the Ponemon Institute, 50% of the respondents perceived third-party access as the fundamental reason behind the increasing number of cyberattacks [37]. A Cyber Risk Report published by the same institute in 2018 lists third party vendor abuse as the second-biggest security threat to the supply chain [38].

One example of third party vendor misuse is the Target Breach of 2014, where the attackers used malware to steal credentials from one of Target's less secure HVAC vendors, and consequently, the attackers gained access to Target's vendor-dedicated Web services [39]. These kinds of attacks have also taken place in various other organizations. For example, JP Morgan fell victim to a data breach following an initial assault on an online platform operated by a third-party website provider. Besides, there are several instances where the company's data was leaked even after the company's relationship with the vendor had terminated. Even though companies follow through with various systems and procedures when an employee is terminated, the same stringent procedures are not followed in case of third-party vendors to prevent the loss of business.

Unfortunately, even with dynamic security controls in place to continuously monitor for threats, the vast majority of organizations struggle with supply chain risk management and remain vulnerable to third-party hacks and breaches [40]. In a 2018 survey, 59% of the companies in the USA and the U.K., acknowledged that they endured a data breach via a third party; still, only 35% of them assessed their third-party risk management (TPRM) program to be adept [37]. To this end, there is a need for stringent procedures to minimize security risks arising from the association with third-party vendors. These procedures can be made clear to the vendors before the start of business, and access to private information should be granted to the vendors only after these procedures are put in place.

IV. SECURITY CRITICAL APPLICATION AREAS OF THE SUPPLY CHAIN

A. Pharmaceutical Industry

Pharmaceutical products form the backbone of any country's healthcare system. Pharmaceutical firms are regularly confronted with diverse security threats, such as cargo theft, counterfeiting, illegal diversion, and adulteration, all of which can serve as an obstacle to a competent health care system and consequently increase the risk to patient's safety substantially [41]. The main security challenges faced by pharmaceutical supply chains are discussed as follows.

1) *Counterfeiting:* Drugs that are fraudulently manufactured or mislabelled in a way that they appear to the customers as legitimate drugs are called counterfeit drugs. The troubling aspect of such fake medicines is that they may contain the incorrect active ingredient, the incorrect quantity of the correct active ingredient, or, in some cases, may not contain any active ingredient at all. This may pose serious threats to the patient's well-being and, in some cases, may even be fatal.
2) *Illegal Diversion:* Drug diversion is the act of defrauding official supply channels to redirect medicines intended for a specific group of consumers to unregulated environments, such as gray markets, where some other group may illegally purchase them [42]. To do this, perpetrators take advantage of places where the medicines

leave the documented chain of custody. Once this chain of custody is compromised, i.e., once a drug leaves its responsible distribution channel, there is no way to guarantee its fitness [43]. The most common example of drug diversion is when a drug approved for sale in a particular country is diverted to other countries where it might not be registered.

3) *Cargo Theft:* Besides illegal diversion and counterfeiting, pharmaceutical supply chains also face the risk of cargo thefts. In many countries, particularly low-income countries, poor roads, slow transit times, and lack of cargo security allows perpetrators to steal drugs very early in the supply chain. The primary issue with such thefts is that some of the stolen drugs are reintroduced back into the legitimate supply chain [43]. The stolen batch of drugs might not be stored, refrigerated, or distributed correctly, thereby compromising their adequacy. Therefore, when such drugs are laundered back into the supply chain, consumers may unknowingly receive ineffective drugs, which can have serious health implications.

Given the high level of interdependence between the participants of a pharmaceutical supply chain, any problem encountered by one participant has the potential to disrupt the entire supply chain. Supply chain disruptions can further have dire implications for pharmaceutical companies. They may lead to 1) a significant dip in revenue of the pharmaceutical firm affected; 2) depreciated stock prices; 3) customer dissatisfaction; 4) more stringent regulatory inspections; and most importantly 5) compromised patient safety [44].

B. Agri-Food Supply Chain

The movement of food from the farm to the end consumer through various intermediaries, such as the distributor, the wholesaler, and the retailer, forms the complete agri-food supply chain (ASC). The modern food production and supply system transcends regional borders and has now become a transnational economic operation.

Owing to the health risks that malignant food products carry, food quality and safety have gained significant attention in recent years. Apart from being a performance measure of its own, food quality is directly linked to other food characteristics, such as integrity, safety, and shelf life [45]. Several attributes of the ASC, such as storage conditions and transportation facilities, have a major impact on the food products reaching the end user.

Therefore, the ASC, like the pharmaceutical supply chain, requires more stringent safety measures as compared to the other supply chains to ensure product safety [46].

Supply chain management is responsible for the efficient movement of products and services from the suppliers to the end user. Supply chain risks tend to impact this process and interrupt the flow of materials as planned. These risks may, or may not, interrupt shipments, trigger delays, or harm the goods in any way [47]. The ASC risks have been perceived as the epicenter of the majority of food problems worldwide. The two kinds of risks that an ASC faces are as follows.

1) Internal risks in normal operations, such as excess inventory, late delivery, inaccurate predictions, human error, minor accidents, and IT system failures.
2) External risks resulting from situations beyond the management's control, such as earthquakes, hurricanes, labor disputes, wars, attacks from pirates or terrorists, epidemics, unusual rise in prices, problems with trading partners, and raw materials' shortage.

ASC risks have the potential to influence the safe operations of the whole supply chain. If the ASC risks can be detected in advance, then adequate steps to mitigate the latent risks of the supply chain can be taken to avoid accidents before they occur. To this end, it is essential to set up an early warning system for food supplies that enhances the standard of food safety measures and limits the risks that food supply chains face. Such an early warning report system can offer vital information for the management of food supply chain risks. Adopting an effective approach to issue early warnings for risk management in the ASC can also help examine the risk factors associated with the chain [47].

An issue in any part of the food chain has the potential to affect the entire food chain; therefore, it is necessary to ensure the proper functioning of each part of the chain. This will limit problems in a specific stage of the chain from flowing into the next link and consequently help eliminate the danger as much as possible at the embryonic stage.

C. Software Supply Chain

A software supply chain extends the notion of a traditional supply chain to software and systems distribution. Although the fundamental business reasoning and significance of adopting a supply chain model remains the same as that for a traditional supply chain, a few differences exist among the two, which are as follows.

Resources Required for Production: The production process is an essential step in the supply chain; without production, there is no product to supply. In traditional industries, the supply chain typically begins with the raw materials used for production and continues with supplier management, distribution, and more. However, in software supply chains, it can be challenging to determine the exact resources needed since a tangible product or service is not being delivered [48].

Distribution: Certain distribution problems are specific to the software supply chain, such as 1) the means to distribute the software to the end user; 2) software packaging and pricing; 3) managing open source components; and 4) addressing the changing needs of customers.

Risks: In addition to risks like counterfeiting, delayed deliveries, individual mistakes, as well as other internal and external risks that traditional supply chains face, a software supply chain has an added risk of incorrect or incomplete code, which makes the chain vulnerable to attacks by malicious entities [5].

End Point: Unlike most tangible products or services, the software supply chain does not end at the point of sale. There might still be a need for maintenance, issuing software updates, releasing new versions, or collecting data. The software supply chain management also needs to ensure that

the customer is paying the ongoing subscription fees and using the software in a way that complies with the licensing agreement [48].

D. Spare Parts Supply Chain

The spare parts supply chain plays an integral role in preserving the machines' operational capabilities; therefore, the shortage of spare parts can have a detrimental impact on various industries. The methods and procedures for managing the supply chain and inventories of spare components are quite different from those for standard goods or services. Spare parts are often associated with high costs, and unlike finished goods, their demand is extremely volatile [49]. The sporadic demand for spare parts makes their demand forecasting a real challenge. Furthermore, the high price of replacement parts often motivates malicious entities to counterfeit these parts for their financial gain. These counterfeit components can pose a severe risk to industries where the working of equipment has a zero margin for error, such as the defense industry, aerospace industry, and the automobile industry. Bodner [50] and Tehranipoor *et al.* [51] showed how pirated parts—whether mechanical, electronic, or otherwise—enter the aerospace and defense supply chains and can jeopardize the quality, reliability, and security of aerospace and defense products. Authentic parts have known production histories and conform to the quality control policies set by the manufacturers, while fake parts are unreliable and have minimal quality controls. The possible repercussions of counterfeit spare parts include equipment malfunction, maintenance issues, lost revenue, exfiltration of electronic data, and risking national security. In aerospace systems, the implications of counterfeit spare parts include the potential loss of whole structures, such as satellites and aircraft.

E. Retail Industry

The retail industry is one of the busiest industries in the world. Retail organizations need to continually innovate their products and shift retail formats to meet the changing consumer needs. Retail organizations are further constrained by their need to take into account the price and quality of their products while ensuring faster deliveries. To this end, the retail supply chain plays a vital role in any retail enterprise's development by helping it create new products and services, improve its productivity, and compete with other organizations. However, for the efficient functioning of the chain, these enterprises need to allow their suppliers and associates access to their systems and certain sensitive information. This can render organizations vulnerable to certain risks, such as misuse of data and lack of organizational privacy [52]. Furthermore, since most retail networks lack a sufficient number of distribution centers, many of today's retail supply chains are cracking under the strain of handling the increasing demand for speed and convenience in a cost-effective manner. Therefore, it has become essential for the retailers to closely monitor the supply chain to ensure that the products being delivered are:

1) free from any defects to minimize customer dissatisfaction [53];
2) accurately labeled and branded to limit processing errors;
3) adequately cataloged in a secure database to facilitate adequate data analysis;
4) tracked properly to reduce the possibility of theft and forgery;
5) always on the move to maintain a low cycle time [53].

F. Oil and Gas Industry

The oil and gas industry continues to have a tremendous influence in global economics and politics, particularly in regards to the employment levels, with the U.S. oil and gas industry supporting at least 10 million workers alone. The U.S. energy information administration (EIA) forecasts that OPEC crude oil production will average 29.2 million barrels per day from April 2020 to December 2020 [54]. This corresponds to a net total of around 10.6 billion barrels per year, a rise of about 41% from 7.5 billion barrels consumed in 2018 [54]. Therefore, the various risks facing the oil supply chain cannot be overlooked. The risks facing the oil and gas supply chain can broadly be classified as follows.

1) *Physical Risks:* Physical threats, such as terrorist attacks on the oil infrastructure, piracy attacks on the vessels carrying oil, and theft from storage warehouses, are the most obvious types of danger to the oil supply chain.
2) *Operational Risks:* Mismanagement in any step of an oil supply chain can severely impact the whole supply chain, and in many cases, it can lead to environmental disasters causing heavy loss of human lives.
3) *Cybersecurity Risks:* In today's world, apart from physical threats, supply chains also face the risk of cyberattacks. These risks emerge because supply chains rely on a range of software and hardware, as well as data collection instruments. Such dependencies open new doors for those who want to manipulate supply chains and get sensitive information.

G. Gold Industry

Gold supply chains are particularly complex, making them prone to a variety of challenges, some of which are mentioned as follows.

1) *Counterfeiting:* Trade of counterfeit gold bars and jewelry has been growing at a tremendous rate. A recent Reuters survey of senior executives at numerous gold refineries uncovered the forgery crisis faced by the world's gold industry. According to the respondents, the quality of forged gold bars has risen considerably in the last few years, making it harder even for the industry experts to distinguish counterfeit gold bars from real ones [55].
2) *Lack of Transparency:* It is essential to have a reliable tracking system in the gold supply chains to monitor gold from the time it is extracted from its ore to the time it is delivered to the end consumer. However, the lack of transparency in the traditional supply chain's tracking system jeopardizes the efficient operation of the gold supply chain. Each participant in the supply

TABLE III
TECHNIQUES AND TECHNOLOGIES ENHANCING THE MODERN SUPPLY CHAIN

	Overview	Benefits	Security Implications
Supply Chain Digitalization [56]–[58]	A fundamental redesign of supply chain processes using modern technologies such as IoT.	The digitalization of the supply chain increases accuracy, agility, and efficiency.	Addition of several unsecured devices, Single point of failure
Circular Supply Chain [59]–[61]	An amalgamation of supply chain management with the concept of the circular economy.	Boosts economic growth by creating more jobs while ensuring greater sustainability.	Management policy failures may have dire financial and security consequences.
Wearables [62]–[64]	Communication enhancing devices that are worn on the body and connected to the internet. Examples include smart glasses, smartwatches, and fitness trackers.	Besides enabling enhanced communication, wearables can augment the safety of the users while also increasing their productivity.	The lack of clear regulatory policies and in-built security features renders wearables susceptible to malicious attacks.
Cloud Computing [65]–[67]	The integration of cloud management solutions with supply chain management has the potential to revolutionize supply chain management.	The use of cloud computing platforms can offer enhanced security, efficiency, and scalability.	Cloud platforms are very often associated with compliance violations and cybersecurity complications.
Big Data Analytics [68]–[70]	The use of quantitative tools to mine information essential for developing new insights.	Big data analytics yields better insights that enable better decision making.	Need for systematic security audits to minimize the risk of a data breach.
Social Media [71]–[73]	By enabling all supply chain participants to monitor supply chain events regularly, social media can allow for a more dynamic supply chain management system.	The use of social media in supply chain management can offer enhanced visibility and facilitate improved communication.	Several cybersecurity challenges, such as malware attacks, data threats hinder the use of social media in supply chains.

chain may know and trust his/her immediate supplier, but the same cannot be said for the supplier's partners. Furthermore, most participants in the supply chain do not have detailed knowledge about the raw material's origin and cannot determine whether the gold has been mined responsibly. This lack of transparency breeds distrust among the supply chain participants, particularly the consumers, which might deter them from buying the end product.

3) *Smuggling:* The smuggling of gold products occurs via the international flow of containers used to transport legitimate gold products. The illegal trade of gold has a significant impact on not only the end consumers but also on other participants in the supply chain. First, smuggling compromises the reputation of the executives that are responsible for managing the supply chain. Second, the high cost of gold products makes their smuggling an attractive prospect for criminals looking to launder their money. Lastly, smuggling begets instability in the local economy, thereby inhibiting business opportunities of legitimate corporations. According to a recent Reuters article, an increasing number of gold bars branded illicitly with the logos of well-known Swiss refineries are making their way into the global market in an attempt to launder forged gold. In the last few years alone, Switzerland's top four gold refineries have identified $50 million worth of fraudulently branded gold bars [55].

The current state of the gold industry has made the task of securing gold supply chains an essential task to minimize fraud and scams. To this end, blockchain poses to be a promising solution. With the exponential rise of blockchain 2.0, blockchain has become more than just a platform for cryptocurrency. Blockchain can be used to monitor both digital and physical goods throughout the chain, as long as all chain-of-custody members have links to a blockchain platform. In the case of gold, blockchain can help in monitoring all the entities from the mine to the factory to the metal manufacturer to the dealer to the seller, and finally to the consumer.

V. IMPROVEMENTS AND ENHANCEMENTS REQUIRED IN THE MODERN SUPPLY CHAIN

As discussed in Section I, the modern supply chain differs significantly from the more traditional supply chain. In this section, we discuss the key technologies that have made the supply chain more efficient and are further expected to transform the shape of supply chain practices (refer to Table III).

1) *Supply Chain Digitalization:* Supply chain digitalization refers to the use of modern technological advances to make the logistics processes more dynamic, fast, and resilient. The digitalization of the supply chain optimizes the supply chain by making it a) faster; b) more flexible; c) more granular; d) more accurate; and e) more efficient [74]. According to the MHI annual report, 80% of supply and manufacturing industry leaders expect digitalization of the supply chain to be standard in five years [75]. However, merely adding the modern technologies and features to the current supply chain model

is not sufficient. Fundamental redesign of the supply chain strategies is required to leverage the real features of digitalization. IoT is the most effective technology for the digitalization of the supply chain. IoT can aid supply chain digitalization by enabling the inventories to automatically request for fresh stocks based on the current demand, previous data analysis, and pending stock without human involvement [76].

2) *Circular Supply Chain:* The traditional supply chain is linear in nature, i.e., the goods are transferred from the manufacturer to the end user and then finally discarded. However, the circular economy is being acknowledged as a better alternative to the prevailing linear economic model. In recent times, the demand for sustainably produced goods has increased, and recycling and reuse of discarded products have become hot topics. The circular supply chain integrates the philosophy of the circular economy into supply chain management, thereby offering a new and compelling aspect to the supply chain sustainability domain [77].
3) *Wearables:* Wearables refer to devices worn on the body that are connected to an Internet source and can be used to enhance communication to and from the users. Wearables range from smart glasses like Google Glasses, smartwatches like Apple Watch and Fitbit to personal sensors. In addition to improving the operational efficiencies of the modern supply chain, wearable technology provides several advantages for the supply chain.
    a) Wearables can allow workers to perform critical supply chain tasks without the need for taking up space or additional resources.
    b) Wearables like smart glasses and voice command devices have the potential to facilitate enhanced communication across the chain. Improved communication can subsequently lead to a significant rise in productivity.
    c) Wearables, such as fitness trackers and smartwatches can monitor employees' health and stress levels via various embedded sensors.
    d) Wearables enabled with GPS technology can easily locate employees and prevent them from entering a restricted zone [78].
    e) Warehouse managers can use wearables to capture stock information quickly and accurately, and to keep track of the products produced, transported, and delivered.
4) *Cloud Computing:* Traditional supply chain management systems are much more transactional and cannot offer the efficiency and accuracy of cloud management solutions. Therefore, most of the large-scale businesses are adopting the use of cloud computing in the supply chain processes. Integrating cloud computing features in the traditional supply chain systems not only allows organizations to accurately track the manufactured products throughout their lifecycle but also ensures rapid scalability and improved security while being cost effective.
5) *Big Data Analytics:* Big supply chain analytics uses data and quantitative tools to improve decision making for all supply chain operations [79]. The vast scale deployment of connected devices, such as trucks, RFID readers, mobile devices, webcams, and sensor networks generates a considerable volume of data. With big data analytics, companies can exploit this data to achieve the attitude, skill set, and technology required to become a data factory. Furthermore, big data analytics can help generate new ways to strengthen the decision-making processes in the supply chain, from improved frontline operations to enhanced policy decisions, such as the selection of the best operating model for the supply chain [79].
6) *Social Media in Supply Chain:* Today, nearly half of the world's population is present on one or the other social media platform. All businesses around the world have understood the power of social media and embraced its engagement in the supply chain. In a survey conducted by IDG Research Services, 57% of the respondents stated that if given a chance, they are open to the idea of using social media in their supply chain [80]. The use of social media can improve supply chain management by enhancing visibility, improving communication, increasing control, and reducing labor and operational costs [73]. The domino effect of using social media to improve supply chain management can span across the entire organization, which can help in enhancing customer satisfaction and claiming the highest customer value.

With the advent of technologies, such as IoT, blockchain, drones, and artificial intelligence (AI), the future supply chain could look entirely different from the current one. Fig. 3 illustrates one potential supply chain scenario as envisioned by McKinsey and Company [74]. The flow of the figure can be better understood by categorizing the supply chain activities into steps.

1) *Advanced Forecasting Techniques*—big data analytics and advanced forecasting techniques that take into multiple factors, such as weather, special events, and rapidly changing marketing trends can enable manufacturers and suppliers to forecast customer demand accurately. In the future, Amazon plans to roll out a system known as predictive shipping, wherein products are shipped even before the customer places an order.
2) *Ad Hoc Planning*—by enabling ad hoc planning, supply chain participants can minimize their planning time and ensure that the products are always on the move. Ad hoc planning can further enable the participants to adapt to dynamically changing constraints (for example, real-time updates on the factory's production capacity and stock availability in the warehouse).
3) *Advanced Transportation Systems*—IoT-enabled vehicles can facilitate real-time tracking and maintenance of the products in transit. Furthermore, in the future, autonomous trucks may become the main mode of shipment owing to their ability to reduce delivery times and human effort.

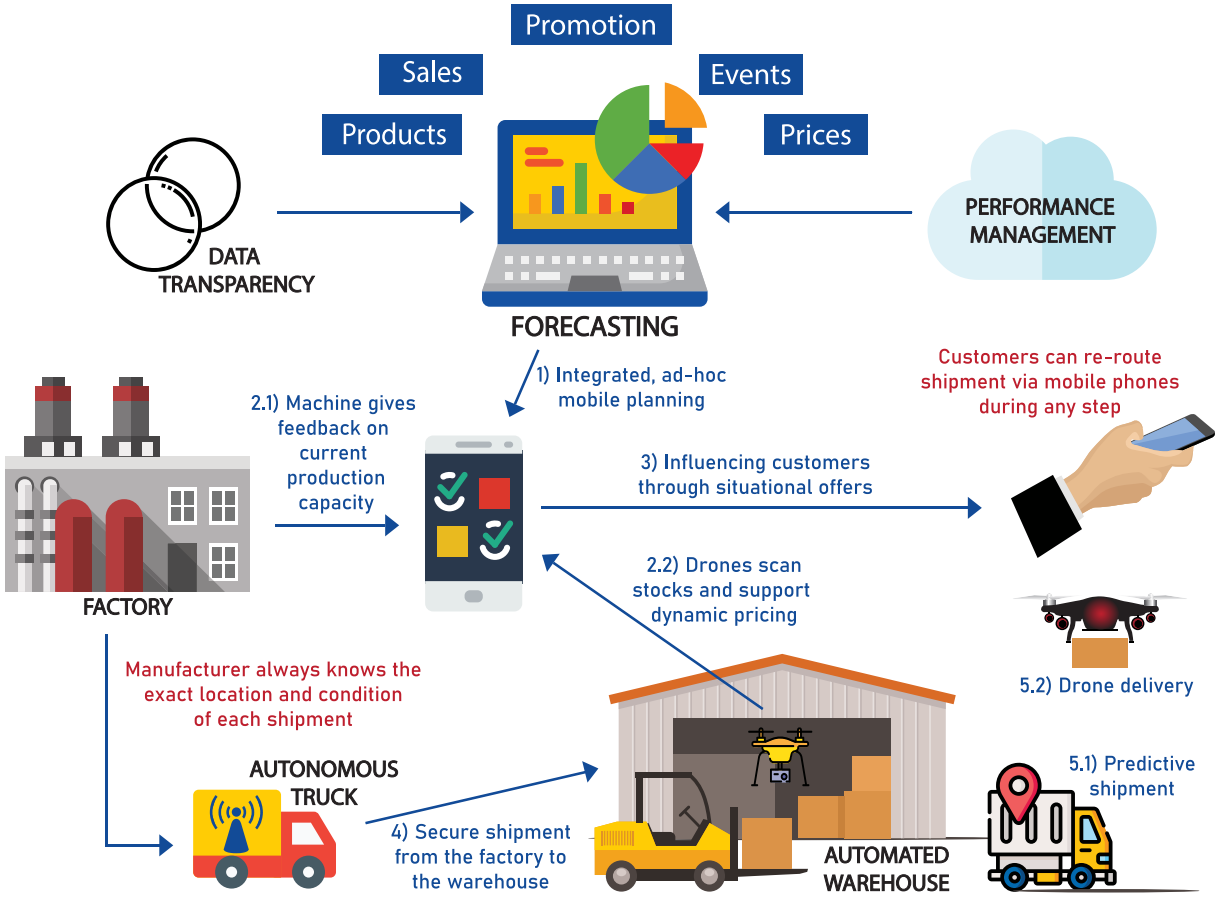

Fig. 3. Future supply chain scenario.

4) *New Delivery Options*—following the COVID-19 outbreak, drones have shown much promise in their ability to act as delivery devices [81]. In the future, drone deliveries may become mainstream allowing customers to choose from a wide array of delivery options. Drone deliveries, in particular, can be used for faster deliveries and also to reach remote places.

VI. Provision of Security for the Supply Chain

The technologies mentioned above, with all their key benefits, have also generated several issues. Such issues at different levels of the global supply chain render it more vulnerable to malicious attacks by adversaries for monetary benefit. In order to maintain a secure supply chain integrated with the technologies mentioned above, there is a need for proper security architectures. To this end, in this section, we discuss a few technologies that have made considerable progress in ensuring supply chain security. Fig. 4 exhibits the recent works done in the domain of supply chain security [82]–[140]. Most of the recent research has centered on the use of three key technologies to ensure supply chain security.

1) Blockchain.
2) ML.
3) PUFs.

The following sections explore ways to integrate these technologies into the supply chain and discuss the role these technologies play in securing the supply chain.

VII. Security Provisioning Using Blockchain

The recent years have seen a tremendous change in the supply chain ecosystem. Consumers nowadays actively pursue brands that can assure their product's authenticity, while other parties involved in the supply chain are increasingly accentuating the need for responsible sourcing and better visibility to minimize conflicts [141]. However, the lack of interoperability and data inconsistency associated with the traditional supply chains has exacerbated the widely held perception that supply chains lack transparency and are inherently complex. The growing complexity of the supply chains and the increasing involvement of various stakeholders has prompted business executives and supply chain managers to seek for a technology that can add new value to the supply chain by overcoming these inefficiencies [142]. By fostering transparency, scalability, and deployment flexibility, blockchain has surfaced as a strong contender for enabling a trusted technology platform required for an efficient supply chain model (refer Fig. 5). Blockchain can facilitate the efficient execution of several supply chain activities, including contractual bids and agreements, product traceability, and supplier payments. Blockchain technology has the potential to become a standardized technology for use in the supply chain by enhancing supply chain security measures, reducing time delays, minimizing costs, and increasing transparency. In this section, we discuss the diverse applications of blockchain technology in supply chain security and management.

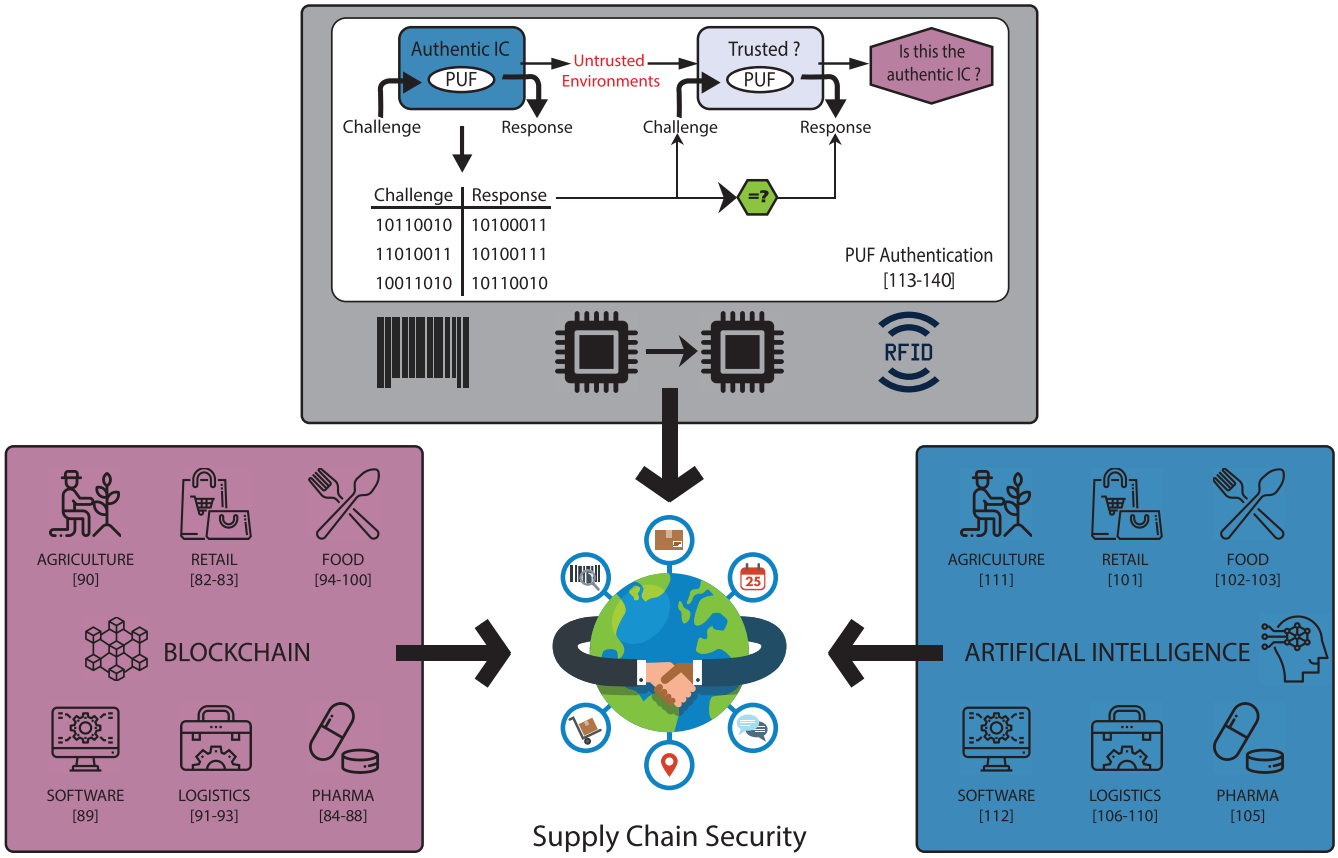

Fig. 4. Works in various domains.

A. Provenance Tracking

Tracking the origin and flow of valuable products, such as electronic equipment, jewelry, artwork, and luxury goods across a supply chain is known as provenance tracking. In today's retail environment, provenance tracking has become an essential task to build trust among consumers. It enables stakeholders in the supply chain to authenticate the products by granting them access to all product-related information. In recent times, blockchain has emerged as an appropriate technology to assist reliable provenance tracking by creating a permanent history of the product from its manufacture to its sale and documenting the transaction every time the product changes hands. Blockchain-enabled provenance tracking could drastically reduce human error, added costs, and time delays associated with the current supply chain transactions. Blockchain technology can facilitate provenance tracking through the following steps.

1) Whenever a valuable article is produced, a corresponding digital token substantiating that article's point of origin is issued by a responsible party.
2) The digital token is transferred parallelly with the physical item, i.e., the real-world chain of custody is entirely mirrored by a chain of transactions on the blockchain [144].
3) The token serves as a virtual "certificate of authenticity," which is considerably more difficult to exploit than conventional authentication methods.

Walmart's Food Supply Chain: Walmart has collaborated with IBM since 2016 to implement a blockchain-based traceability system named "Food Trust System" in their food supply chains. This system has been built on top of Hyperledger Fabric, an open-source blockchain framework housed under The Linux Foundation [145]. The viability of Walmart and IBM's joint venture was analyzed using two proof of concept (PoC) projects—one involving the pork supply chain in China and the other involving the mango supply chain in the U.S. In China, the blockchain-based ecosystem allowed Walmart to bring more trust to the supply chain by enabling supply chain participants to upload certificates of authenticity to the blockchain. In the case of the mango supply chain in the U.S., blockchain reduced the time required for tracking the origin of mangoes from seven days to almost 2 s.

Recently, following the E. coli bacteria outbreak in the romaine lettuce, Walmart made it mandatory for all its lettuce suppliers to be a part of its blockchain-based traceability program. Although the outbreak transpired in just one region, all Walmart stores in the U.S. were forced to remove lettuce from their shelves. This safety measure became a must since it would have taken Walmart stores as much as a week to trace the origin of the lettuce available [146]. However, now, with the Food Trust System in place, all Walmart stores can easily trace a product's origin in mere seconds, thereby alleviating the risk of such issues in the future. Using this system, Walmart and IBM now trace over 25 products, including green

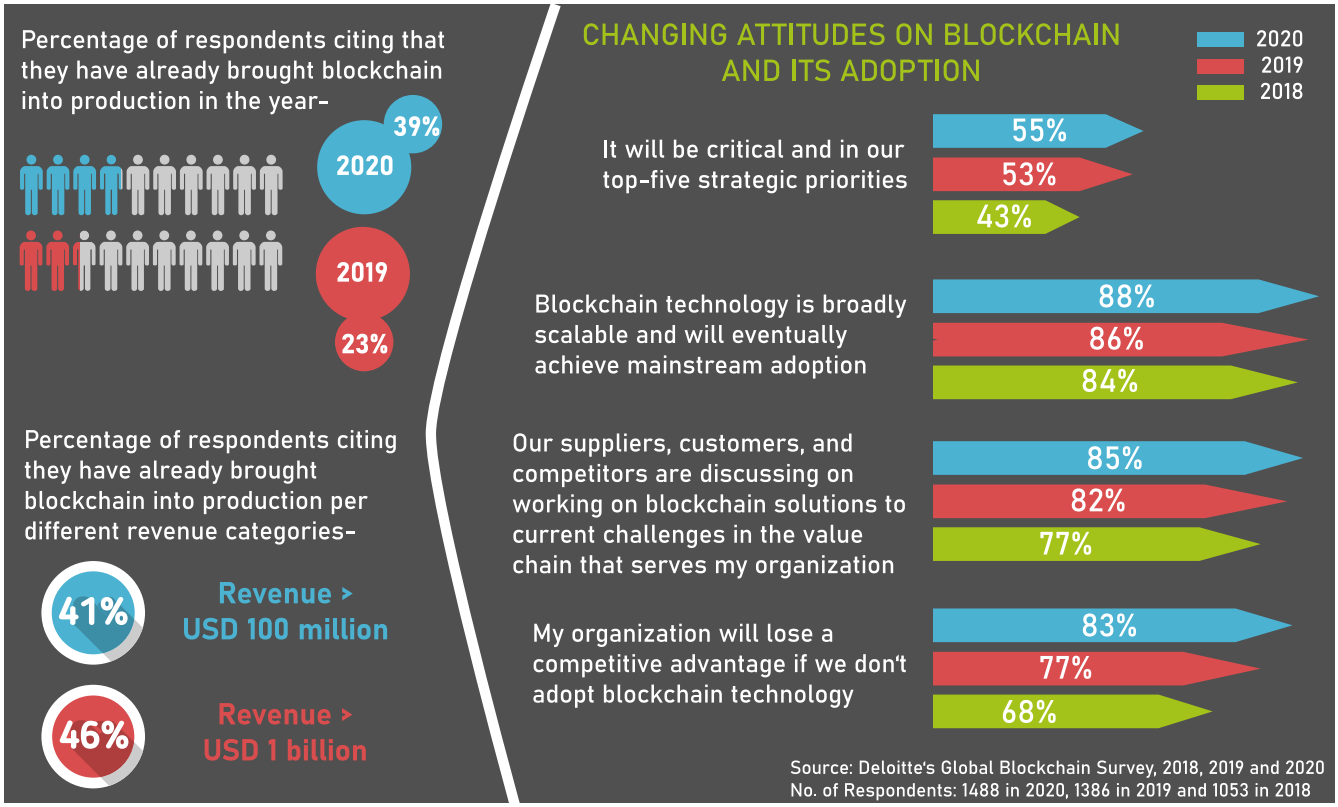

Fig. 5. State of blockchain in the enterprise (Data source: Deloitte, 2020) [143].

vegetables, such as spinach and lettuce; fruits, such as strawberries and mangoes; dairy products like almond milk and yogurt; and poultry, such as pork and chicken [147].

B. Managing Logistics

Today's supply chain networks still depend on the trail of physical documents, which limits the visibility of the products' shipment status among supply chain participants [148]. Coordination among the manufacturer, suppliers, importers, distributors, and logistic partners is fundamental to the efficient management of the supply chain. However, traditional supply chains lack a common data-sharing platform, which makes it hard for the supply chain participants to exchange information [149]. To this end, using a distributed ledger technology (DLT), such as blockchain, is a highly promising solution. A shared platform based on the blockchain technology can:

1) maintain the latest record of the number of assets, such as containers and trailers available, by tracking their movement between the supply chain nodes;
2) foster increased visibility and transparency amongst the supply chain participants by ensuring that all participants have access to accurate and real-time information;
3) streamline the logistics operations by enhancing the level of communication and data sharing among all supply chain participants;
4) optimize logistics costs by eliminating the need for intermediaries and eliminating the possibility of fraudulent transactions;
5) reduce paperwork delays by automating supply chain processes;
6) make supply chains more secure by allowing logistics companies to monitor the shipping conditions and take precautionary action against malicious activities, such as cargo theft and counterfeiting.

TradeLens—A Blockchain Initiative by IBM: TradeLens, a joint initiative by IBM and GTD Solution Inc., is an open supply chain platform built on top of a blockchain. TradeLens leverages open source technologies and publicly available APIs to allow third parties to build and deploy applications, thereby fostering supply chain innovation. The main objective of TradeLens is to reduce friction in global trade by digitizing and automating cross-border supply chain operations. The use of blockchain architecture allows TradeLens to enable secure information sharing and collaboration among supply chain participants, reduce delays, and minimize trade documentation [150]. Launched in 2018, TradeLens already has 94 participants, including several ocean carriers, freight forwarders, custom officers, port operators, and government authorities [148].

C. Automating Contracts and Supplier Payments

Even today, numerous companies rely on manual invoicing systems that are inherently inefficient in terms of both time and cost. Additionally, most companies depend on conventional agreements that require third party involvement and a manual check of terms and conditions. Smart contracts deployed on a blockchain network can overcome such inefficiencies by

automating the invoicing process and digitizing the contractual agreements. In essence, a smart contract is a software program that carries all the contractual terms between two or more parties [148]. A smart contract acts as an independent node on a blockchain network and functions only according to some preprogrammed criteria, thereby eliminating any possibility of fraud, bias, or some other interference [151].

A smart contract deployed over a blockchain-based network of supply chain participants can enable the enforcement of payment terms and other predefined conditions [152]. For instance, smart contracts can initiate payment on the successful completion of a trade provided that the supplier presents evidence of the same. Conversely, if the payment is required to be carried out before the delivery, smart contracts can withhold delivery until a receipt of the payment is received and verified. If the delivery or the payment does not meet the predefined criteria, the smart contract can trigger some sort of a sanction [146]. Furthermore, smart contracts can also help in maintaining data consistency across all supply chain stakeholders and eliminate costly errors. For example, conventional systems might fail to identify a duplicate or slightly inaccurate invoice sent by a supplier. However, a blockchain-based contract that maintains all the past transactions and analyzes all the aspects of the invoice will automatically discard the duplicate/erroneous invoice.

Smart Contract Application by Adapt Ideations: An IoT centered innovation agency known as Adapt Ideations has recently developed a smart contract application on top of IBM Hyperledger. The main objective behind this endeavor is to eliminate costly delays and digitize all paperwork. As a PoC, Adapt Ideations drafted a smart contract between four supply chain participants and deployed it on their blockchain platform. The company's IoT sensors provided the blockchain platform real-time updates in regards to temperature and operating time of the machines being monitored. Any discrepancy in any of the parameters triggered the smart contract, after which all the supply chain participants were notified of the issue. Following the success of its test project, the company is now working on making the platform more advanced in terms of scalability and robustness. According to the company's claims, the company's blockchain platform, in tandem with its IoT sensors, has the potential to automate most of the supply chain operations [153].

D. Limiting Supply Chain Disruptions

The impact of the recent COVID-19 pandemic has highlighted the fragile nature of supply chains. Amid such emergencies, most businesses worldwide find it hard to maintain the flow of their goods and services. Further aggravated by trade restrictions, supply chain disruptions caused by such emergencies force a majority of manufacturers to limit, and in some cases, shut down their production [20]. Subsequently, many logistic partners are compelled to limit their shipping capacity, which leads to a shortage of both essential and nonessential goods [154]. Maintaining robustness, agility, and transparency in supply chains is essential to limit such disruptions. However, traditional supply chains tend to lack these characteristics. The lack of transparency in conventional supply chains limits manufacturers' knowledge regarding the challenges faced by their suppliers or their supplier's partners. Awareness about such challenges can empower manufacturers to arrange for interim solutions to minimize disruptions in the supply chain. To this end, blockchain technology can play a pivotal role in transforming the trade networks by making them more secure, visible and transparent [20]. Permissioned blockchain ledgers, in particular, can facilitate the secure transfer of knowledge within the supply chain while ensuring complete anonymity. Adopting blockchain technology can further enhance supply chain agility and robustness by 1) eliminating the need for mediators; 2) reducing the time required for intermediate transactions from days to minutes; 3) making the supply chain more streamlined; and 4) automating the deployment of contractual relationships.

LeewayHertz's Blockchain-Enabled Agri-Food Supply Chain: A blockchain-development startup named LeewayHertz has proposed a potential blockchain-based solution to overcome the multiple issues prevalent in the traditional ASC, such as inefficient logistics processes, limited transparency, the threat of illegal diversion and the risk of food-borne illnesses. Fig. 6 illustrates the startup's proposed ASC [155].

1) *Farmers:* In the chain, farmers use a mobile app to store their food crops' details on the blockchain, which can be accessed by all stakeholders in the supply chain. Farmers also upload the pictures of their crops to allow supply chain stakeholders to evaluate their crops' quality using computer vision (CV) techniques. A smart contract deployed on the blockchain network will further check the compliance of the crop's data with preprogrammed conditions.
2) *Food Refineries:* Upon successful examination, food processing companies bid for the crops via the smart contract. Once the bid is accepted, the farmers are required to distribute the crops to food processing companies. Like the farmers, the food processors also store the information regarding the refining of crops on the public ledger. The smart contract deployed on the blockchain network ensures that food compliance is followed during all the refining processes.
3) *Wholesalers:* Wholesalers bid for the processed products through smart contact, following which the food refineries transport their food products through IoT-enabled vehicles. The IoT sensors embedded in the vehicles enable the real-time GPS tracking of the vehicles and also ensure that sufficient temperature conditions are maintained inside the vehicles for the safety of food items.
4) *End Consumers:* The details of all the steps involved in the production of the final food product are digitally linked to the public blockchain. At each step, these details are validated by all the supply chain stakeholders to reach a consensus. Following the validation process, these details are added to the ledger as an immutable record. An end consumer can easily check for the product's authenticity, its quality standards, and its

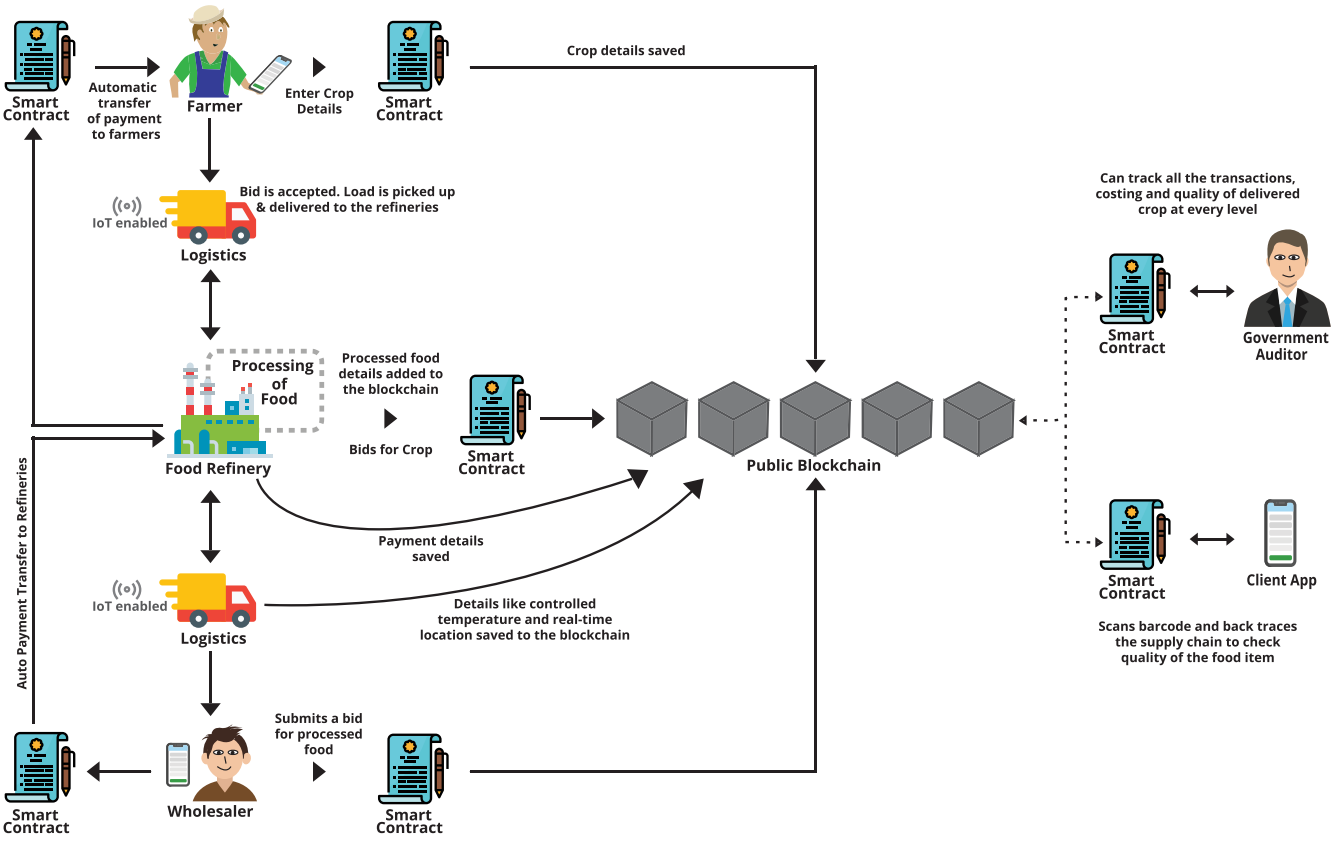

Fig. 6. Security of ASC using blockchain.

safety. Besides, the blockchain network can also enable certain government auditors to perform audit checks on the quality of the food to ensure that the product is safe.

In the past few years, many startups and established enterprises have adopted blockchain-based solutions in their supply chain, and before long, as experts suggest, blockchain could become the "supply chain operating system" [156]. However, it is important to note that a blockchain venture cannot be adopted unilaterally. A distributed ledger inherently requires cooperation between multiple parties, whether it is used for provenance tracking or for automating supplier payments using smart contracts [146]. Therefore, any organization company looking to adopt the blockchain technology needs a well-planned strategy to ensure a smooth collaboration between all of its supply chain partners.

VIII. How Is AI Revolutionizing the Modern-Day Supply Chain?

In recent times, AI, particularly ML, has become a major technology to enter all the key domains, including logistics and supply chain. The primary reason for AI's successful adoption in the supply chain is attributed to its potential to simplify complex supply chain processes. As per McKinsey's estimates, the use of AI in supply chains can help enterprises gain an economic benefit of up to $2 trillion annually [157]. Furthermore, 63% of the respondents to a recent survey conducted by the same organization, i.e., McKinsey, report an increase in revenue from AI adoption in their business units, particularly in marketing, product development, and supply chain management [158]. In this section, in addition to the security-enhancing applications of AI, we discuss the various ways in which it is revolutionizing supply chain management).

A. Demand Forecasting

Supply chain planning and management are heavily reliant on proper demand forecasting. Although demand trends of everyday products, such as food remain more or less consistent, demand uncertainty can be high in lifestyle products, such as clothing and technology. Demand forecasting allows supply chain managers to plan productive business activities, optimize inventory levels, estimate potential risks, manage demand exceptions, and formulate mitigation strategies [160]. However, the use of inefficient demand forecasting strategies can also lead to incorrect forecasts that can further translate into significant financial losses for organizations. For example, in 2001, Nike's failed attempt at implementing a demand-forecasting software in its supply chain resulted in an understock of the in-demand Air Jordans and an overstock of relatively unpopular shoes [161]. This fiasco caused a huge financial blow to Nike, with sales losses amounting to around $100 million. In recent years, supply chain officials have relied on several methods, including historical data analysis, live data analysis, linear programming, ML algorithms, and other time series analysis methods to enable real-time demand forecasting. Insights from such models can help enterprises

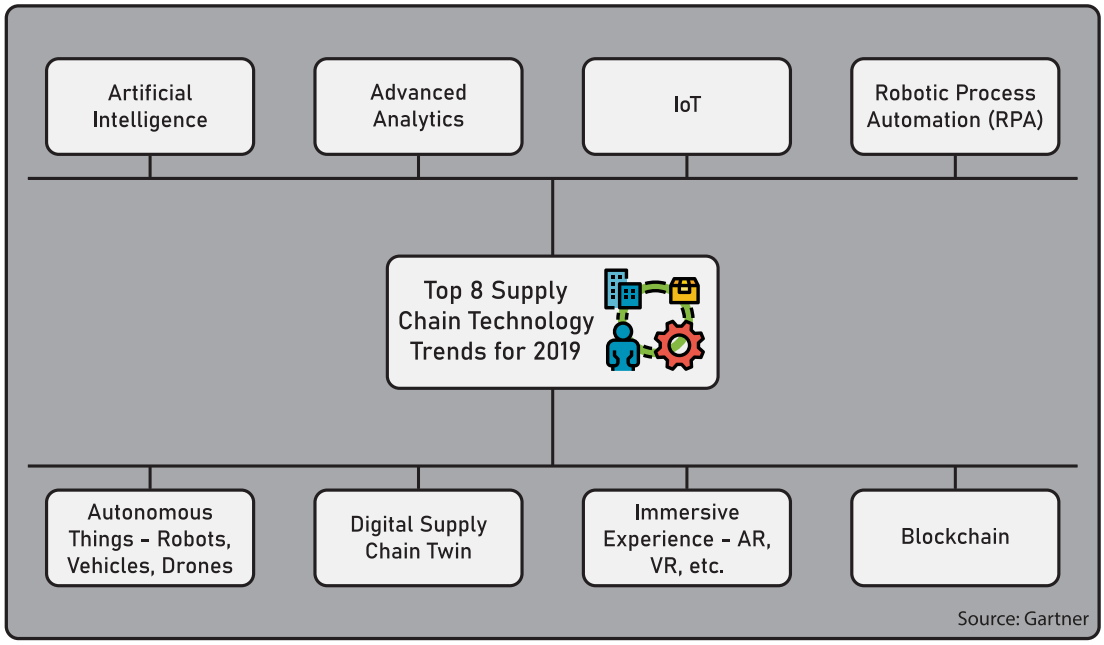

Fig. 7. Top 8 supply chain technology trends—2019 (Source: Gartner [159]).

in accurately determining the supply volume in advance and developing dynamic operational strategies.

B. Inventory Management

An essential component of supply chain management, inventory management is defined as the process of supervising the flow of goods from the manufacturing plant to the storage facilities and from these facilities to the retail stores. It is important to note that demand forecasting and inventory management are closely related. If the supplier fails to meet the consumers' demands, the company's time and money go to waste while also causing customer dissatisfaction. Alternatively, if the supply is much higher than the demand, critical resources are exhausted for no additional profits considering no opportunities are available for selling the overstock. According to some highly regarded business consultants, high inventory levels are one of the main issues that impede the profitability of organizations [162]. Besides, as interest rates gradually rise, inventory storage costs also increase [152]. ML techniques can mitigate such risks by accurately determining the supply volume in advance and developing dynamic operational strategies. ML and data analytics techniques can provide powerful insights that can help in labor management, automating inventory systems, optimizing vehicle deployment strategies, and enhancing the agility of supply chain decision making.

C. Automating Processes Using RPA

Many businesses worldwide spend a considerable amount of time, money, and human capital on repetitive supply chain processes [163]. According to a 2017 study conducted by the Tungsten Network, businesses report that, on average, they spend about 125 h every week on insignificant business activities, such as responding to supplier inquiries and handling international taxes and invoice frauds. This corresponds to a yearly gross of 6500-h wasted processing trivial tasks [164]. To this end, many businesses are employing robotic process automation (RPA) and other technologies to help in automating repetitive tasks. Furthermore, the adoption of ML algorithms in RPA has made software robots more intelligent and flexible. The use of these algorithms can also help determine the robots' working strategies and update them automatically based on the environment. RPA's inclusion in Gartner's top 8 supply chain technology trends is a testament to its increased adoption in supply chain management (refer to Fig. 7).

D. Chatbot for Enhanced Customer Support

Chatbots, also known as conversational agents, are making strides in enhancing customer support. Chatbots can handle many trivial tasks efficiently, therefore eliminating the need for customer support personnel. In recent years, chatbots powered by ML techniques like natural language processing (NLP) and voice recognition have redefined the relationship between logistics providers and customers by tailoring support to customer needs. According to Accenture estimates, chatbots have the potential to manage 80% of all customer engagements [166]. Logistical chatbots can:

1) enable customers to submit delivery requests;
2) integrate tracking numbers to unique customer IDs to assist personalized planning and shipment tracking;
3) manage customers' orders, including new orders, delayed orders, canceled orders, unclaimed order, orders in progress, and orders for replacement;
4) provide an automated approach to managing the company database by sending real-time updates about each order and delivery to the database;
5) enable fleet management by maintaining details about the delivery/supply fleet, for example—the number of

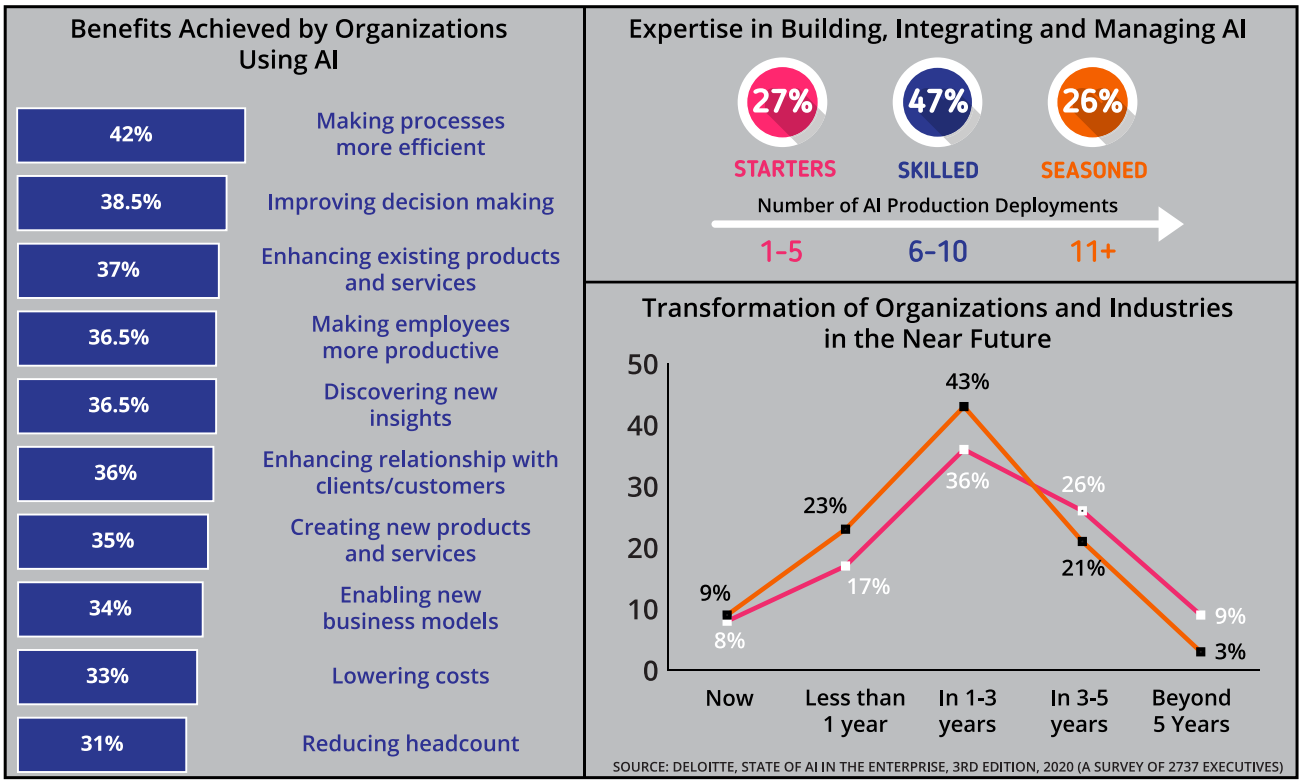

Fig. 8. State of AI in the enterprise (Data source: Deloitte, 2020) [165].

total vehicles, deployed vehicles, available vehicles, out-of-order vehicles [167].

In a recent Deloitte survey of 2737 company executives, about 36% of the respondents said that AI played a significant role in enhancing their relationship with their clients, while around 42% said that AI made otherwise complex processes more efficient (refer to Fig. 8).

E. SVM for Risk Analysis

In recent years, the management of supply chains in a way that secures them against disruptions by anticipating their occurrence and minimizing their antagonistic effects has become a hot topic [168]. To this end, Camossi *et al.* [169] realized the importance of developing risk analysis tools aimed at detecting suspicious containerized transports. The authors propose a support vector machine (SVM)-based framework named anomalous container itinerary detection (ACID) to evaluate container system messages (CSMs) and subsequently discover abnormal container shipments. ACID encompasses a preprocessed module whose function is to segment the CSMs into container itineraries, post which they are analyzed to detect any abnormalities. After identifying the irregular container shipments, customs authorities can be notified about the suspicious routes for further investigation.

F. Transit Monitoring With AI-Powered IoT

In recent times, the use of AI in logistics and shipping has become critical within supply chain management. Technological advancements in the telecom industry have made the data collection processes easier, thus warranting the adoption of data mining techniques and pattern recognition techniques to augment existing predictive maintenance strategies. Predictive maintenance not only helps to reduce labor costs and transport time but also ensures safe transfer of goods. With a paradigm shift from product to service-based operations, more and more industries are realizing the importance of predictive maintenance.

Technologies like GPS, GPRS, RFID, and GIS are assisting real-time tracking of shipping vehicles, which is crucial in monitoring the transit of goods and detecting issues, such as delivery delays. The data obtained from real-time vehicle tracking can be used for the optimization of predictive maintenance techniques. For example, IoT sensors onboard vehicles monitor various parameters, such as fuel level and temperature, which allows the concomitant AI models to detect anomalies and provide real-time updates for avoiding accidents and addressing other safety threats. Furthermore, insights about traffic congestion can be obtained using deep learning models applied to video surveillance. These insights can allow supply chain managers to save fuel and time by dynamically analyzing traffic patterns and planning supply routes accordingly.

G. Supplier Selection

Sourcing from the right suppliers has become an increasingly important concern for improving the quality of decision making and consequently enhancing supply chain sustainability. Factors, such as the history of the suppliers' delivery performance, audits, and credit scores act as vital criteria for

selecting the right supplier. In recent times, AI has emerged as one possible solution for assisting companies' supplier selection procedure. In particular, ML algorithms based on historical data have enhanced the supplier selection process by making it more predictive and intelligible [170]. For example, Nodeh *et al.* [171] proposed a novel object-oriented framework to aid optimal supplier selection in petroleum supply chains. This model leverages data mining and neural networks techniques to reduce the time delays, cost, and human errors prevalent in existing selection models. As per the published results, this model leads yields better accuracy as compared to several other supplier selection procedures.

H. Autonomous Vehicles for Secure Shipping

In the present scenario, aside from driving, drivers are responsible for various miscellaneous activities, including documentation, inspection of the vehicle, and planning the route. This leads to a significant wastage of time, money, and human resource. Furthermore, traffic law violations, operational errors, or simple carelessness are responsible for the majority of traffic accidents. To this end, autonomous vehicles have the potential to make a significant difference due to their ability to move safely by sensing their environment and making decisions intelligently with little to no human involvement. In comparison to human driving, autonomous vehicles have the following advantages.

1) They can measure the environmental factors quickly and accurately, making the vehicles' response time much shorter.
2) They can eliminate the issue of the "blind zone" while driving.
3) They have the potential to standardize driving behavior.
4) With autonomous vehicles, situations of driver fatigue and laziness cease to exist.

For example, autonomous ships have the potential to optimize the global shipping process by lowering fuel consumption and transport costs. According to EU data, human errors account for over 60% of all shipping accidents at the seas; therefore, a global network of connected unmanned vessels, capable of communicating and exchanging data with each other, has the potential to enhance the navigation process and thereby reduce the number of accidents at sea. Such unmanned ships can either be operated remotely like drones (with human control) or self-drive autonomously like driverless cars (with AI and no human intervention).

IX. PUF for Supply Chain

In recent years, the growing popularity and economic importance of electronic devices have provided criminals with an added impetus to sell counterfeit electronic devices [172]. Most of the online retail platforms and the physical retail stores around the world are flooded with counterfeit SSDs, laptops, music players, phones, and much more [122]. Counterfeiters can surreptitiously introduce such counterfeit devices into the supply chain or sell them directly to consumers resulting in the delivery of inferior and nonfunctioning devices to the end users, which consequently builds a feeling of discontent among them.

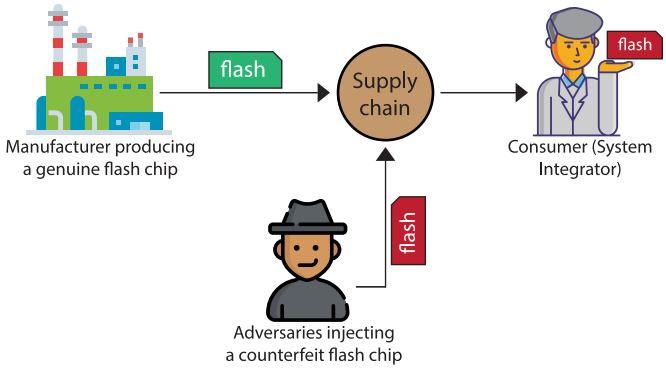

Fig. 9. Threat model for a counterfeit flash chip.

To understand how counterfeit products are injected into the supply chain, let us consider an example of a counterfeit flash chip given by Prabhu *et al.* [122] (refer to Fig. 9). The figure shows that even though the manufacturer produces genuine flash chips, the customer, in this case, the system integrator, ends up buying a counterfeit one. This is because a malicious intermediary injects an artificial chip into the supply chain, thereby compromising it.

In recent years, the trade of counterfeit goods has risen considerably (refer to Section I-A). Much effort is being made in academia and industry to develop effective mechanisms to solve the issue of counterfeiting in supply chains. Physical/PUF, commonly referred to as PUF, has been identified as a useful anti-counterfeiting technology. PUFs are security primitive physical devices initially introduced by an MIT graduate student as part of his doctoral thesis [173]. They are capable of producing a hardware-based digital signature that serves as a unique identifier for each device [123]. By design, PUFs are almost impossible to forge, even by the manufacturer. Therefore, PUFs provide a high level of security to any physical structure within which they are implemented [174]. In recent times, several researchers have leveraged PUFs in a variety of fields. For example, Gope *et al.* [133] have proposed a PUF-based authentication scheme for added security in IoT-enabled healthcare systems. Gope and Sikdar [134] have used a doubtle PUF mechanism for physical security of UAVs. In coming times, PUFs are slated to become a foundational element of supply chain security systems owing to their ability to provide a unique authentication mechanism [175]. In this section, we thoroughly dissect the ways in which PUFs can help to detect and, consequently, deter forgery.

A. Entity-Authentication Using PUFs

Over the years, PUF has been extensively studied as a technique for authenticating devices and entities [124]–[132]. Almost all authentication protocols are typically composed of two stages.

1) *The Enrolment Stage:* Before the registration of a new entity, the unique challenge-response data (CRD) from the entity's PUF is gathered by a trusted party, which

then stores it in a database along with the ID of the entity itself.

2) *The Verification Stage:* In this stage, the trusted party receives the ID of the entity to be authenticated, following which it retrieves the corresponding CRD from the database. A challenge corresponding to the randomly selected challenge-response pair is then sent to the entity. Finally, the entity uses its PUF to calculate the response to be sent back to the trusted party. The entity is considered to be authentic only if the response sent by it matches the one that is stored in the database; else, the authentication fails [123].

One such example of a device authentication scheme can be found in [135]. This article introduces a simple anti-counterfeiting mechanism using static random-access memory (SRAM) PUFs. The authors have built on existing test methodologies to propose the amalgamation of their mechanism into the manufacturing environment. The primary advantage of their mechanism is that it eliminates the need for maintaining an online database while also removing the need for online authentication. Furthermore, according to the authors, their mechanism can be implemented at almost no additional cost within SRAM-embedded devices.

Another example of a PUF-based entity-authentication scheme is presented in [136]. Unlike most of the existing work in the direction of PUF-based entity authentication, the model presented in this article does not endeavor to build a new challenge/response PUF circuit. Instead, the proposed approach attempts to limit the availability of challenge/response pair (CRP) material by employing the use of a "server-managed CRP." Essentially, the motive of the authors is to develop a scheme wherein adversaries with advanced ML capabilities cannot acquire new CRPs without the consent of the server. To achieve this, the authors introduce a lockdown protocol within their PUF-based lightweight authentication scheme. The lockdown protocol puts an upper limit on any adversary's capability in terms of the CRP content accessible. As per the authors' claims, this scheme is compatible with nearly all the PUFs.

B. PUF-Enabled "Unclonable" RFID ICs

RFID is a technology that uses radio waves to automatically capture information stored on a tag attached to an object. RFID technology can enable supply chain managers to uniquely identify distinct physical products and track their movement while also serving as a potential anti-counterfeiting mechanism. Unlike most other measures against counterfeiting, such as tamper-evident seals, holograms, or special printing, RFID does not slow down the supply chain throughput as it does not require any manual intervention. Besides, RFID integrated circuits (ICs) can effectively integrate themselves into any automated system while leveraging the economies of scale and cost reduction curves associated with the manufacture of electronic components [137]. However, even though RFID is an ideal technology to interact with surrounding objects, it has certain limitations in its use as an effective measure against counterfeiting. Some of these limitations are mentioned as follows.

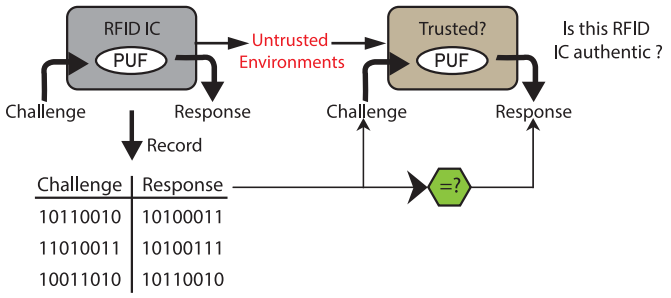

Fig. 10. Overview of the PUF-based RFID authentication procedure [137].

1) *Spoofing:* It is defined as the process of acquiring tag data from legitimate sources using malicious means and transmitting it to a reader [176].
2) *Cloning:* A highly motivated malicious entity can readily generate duplicate RFID tags indistinguishable from the original ones. This is done by copying the original tag's contents and reverse engineering all its properties, including its secret keys [177].
3) *Other Security Threats:* Other possible threats to the security of simple RFID ICs include sniffing/eavesdropping, unauthorized tracking, man-in-the-middle attacks, and Denial-of-Service (DOS) attacks.

To overcome these limitations and optimize RFID's anti-counterfeiting capabilities, there is a need for secure and cost-effective technology. To this end, the authors of [114], [137]–[139] and [178] have proposed the incorporation of PUFs into the RFID ecosystem. PUFs provide a secure, robust, and low-cost mechanism to authenticate silicon chips by exploiting the inherent variations in the IC manufacturing process. This makes PUFs a highly lucrative option for secure authentication of RFID ICs. According to Devadas *et al.* [137], PUF-enabled RFID chips would have their unique secrets, which would be 1) impossible to control before the chip's manufacture and 2) impossible to clone or replicate from one chip to another. Fig. 10 demonstrates their model's PUF-based authentication process for anti-counterfeiting. Following comprehensive testing of their model, the authors have asserted that PUFs can securely authenticate RFIDs with limited overhead.

C. IC Traceability Based on Blockchain and PUFs

To alleviate the risk of circulation of counterfeit electronic devices and to maintain the integrity of the supply chain, it is essential to develop efficient traceability solutions that enable customers to trace the origin of a device. To this end, Islam and Kundu [140] have proposed a novel IC traceability scheme that leverages the use of blockchain pegged to an embedded PUF. In their scheme, a blockchain-based database is used to record and maintain all the details concerning the transfer of ownership. The inherent immutability feature of blockchain ensures that no malicious party can modify or dispute the authenticity of the recorded information. Considering that a transaction record is not sufficient to verify an IC's origin, the authors have employed a PUF to securely bind an IC's identity to the record stored in a blockchain database. The

proposed approach also involves the development and deployment of an ethereum smart contract to automate hardware and software protocols by enabling all supply chain participants to authenticate, monitor, and provision chips throughout their life cycle. While the authors focus on the security of an IC supply chain, it is important to note that this model can be extended to any electronic device supply chain.

X. Discussion, Open Issues and Research Opportunities

A. Discussion

The advent of new and emerging technologies, such as IoT, cloud computing, 5G, blockchain, and AI has piqued the interest of academia and industry alike. In recent times, much research has been conducted around the world to adapt these technologies in different domains and to evolve these technologies further. This section presents a brief discussion on some of the points that need to be addressed when opting for these technologies.

1) While these emerging technologies have tremendous potential on their own, they must be used in tandem with one another to be termed as completely transformative. For example, the existing and emerging IoT applications will be extensively benefited by the arrival of low-latency 5G networks. Similarly, AI with IoT or AI of things (AIoT), gives a whole new dimension to existing IoT devices. This coupling gives existing IoT devices an added capability to analyze data and act on it without human involvement [179], [180]. The association between such technologies can have an enormous impact in various domains like healthcare [181], retail, intelligent transportation systems [182], etc. However, to facilitate the efficient development of such associations, there is a need for dependable performance and interoperability standards [183].
2) While looking at IoT and AI-based systems for supply chains, it is imperative to ensure efficient resource allocation and secure data transmission between the systems at the edge and the cloud [184]. Exposure of confidential data to malicious parties can give rise to network intrusion problems, which can lead to huge financial losses for the organizations[185]. Consequently, it is vital for organizations to ensure stringent data transmission protocols [186].
3) Most ML applications face a tradeoff between learning cost and performance. For example, complex neural network models require higher computational capacity and are therefore costlier than simple regression or classification models but often provide much better results. These applications also face a tradeoff between latency and performance, with weak learners having lower latency when compared to strong learners but suffering in terms of accuracy [187]. To this end, people in charge of developing and implementing such applications have to decide whether they want their data to be sent to the cloud directly (better results) or to be processed at the edge itself (lower latency) [188].
4) Another critical discussion regarding supply chains is the subjective requirement of each industry. Some supply networks like ASCs are more concerned with the delivery time associated with the products in question. However, for other chains like electronic supply chains, a more reliably driven supply chain trumps the latency needs. In the quest for a specific feature/attribute, organizations often have to compromise on other features. Therefore, organizations should have a clear understanding of the industry requirements while making such a decision.

B. Issues and Challenges

This section addresses the performance and safety concerns in the adoption of blockchain, ML, and PUFs that are yet to be resolved.

1) *Blockchain:* While the adoption of blockchain in supply chain management can prove beneficial, its implementation is plagued by several challenges, a few of which are mentioned as follows.
   a) Blockchain implementation in the supply chains requires a complete overhaul of the existing architecture.
   b) There is a vast disparity between blockchain's current capabilities and the capabilities that supply chains need.
   c) Although the tamper-proof feature of blockchain makes it resistant to unauthorized changes, it also makes it impossible to update or delete an incorrect record. This unavoidably leads to the collection of a lot of garbage data, which significantly impedes the application's overall performance.
   d) In comparison to traditional databases, blockchain applications require more storage capacity since they need to record every transaction. Furthermore, the current consensus algorithms used by most blockchain platforms require high computational resources, which can add considerable overhead to the supply chain.
2) *Artificial Intelligence:* The success of an AI solution, particularly an ML solution, depends significantly on the quality of data and the choice of the ML algorithm. The lack of access to useful data may lead to incomprehensible or incorrect results. Similarly, the selection of an unsuitable algorithm may also lead to inaccurate results. The ethics and explainability of the complex AI approach is another significant concern that organizations need to take into account. Until now, several neural networks and other prediction models have been black boxes. There has been little transparency and accountability in terms of training data used, hyperparameters set, optimization functions deployed, among others. Moving forward, organizations should practice and encourage the use of explainable and responsible AI.
3) *PUFs:* The effectiveness of monitoring products in supply chains by the use of PUFs depends solely on the ease with which a malicious entity can counterfeit objects

without affecting the PUF itself. The entire counterfeit detection process can be undermined if an adversary is capable of extracting a PUF from an object and installing it within another. Therefore, the supply chain managers have an additional burden to investigate the feasibility of embedding PUFs within products in a manner that preserves their properties. Other significant concerns associated with the use of PUFs are the lack of reliability and security. PUFs are sensitive to aging and many operating conditions, such as temperature and power supply noise [189]. Besides, the vulnerability of PUFs to modeling attacks renders them prone to several security challenges [190]. To this end, there is a need to overcome the reliability and security pitfalls of PUFs in a cost-efficient manner.

C. Research Opportunities

1) The existing research on logistics and distribution is limited to goods that have a short-term life, such as cosmetics, electronic goods, and pharmaceuticals. In the future, research works in the domain of supply chain management might cover city logistics, emergency logistics, and ASC.
2) The lack of annotated data of admissible quality is a problem for several ML applications. To this end, data augmentation techniques, transfer learning, and domain adaptation are some fields within AI that the community should aim at in the near future.
3) Supply chain security is a vast domain, and with the adoption of IoT, cloud computing, AI, and other emerging technologies, it has become even more complicated. To this end, there is a need for a thorough reference model for future security developments, so that innovations in supply chain security applications can be easily identified, exchanged, analyzed, and exported.
4) Data analysis in near real time is vital for the successful deployment of ML applications in the supply chain domain. This gives rise to the need for advanced ML algorithms to analyze the data at the edge itself. It is also important to note that these techniques should take into account data confidentiality and user privacy. In recent years, a new privacy-preserving ML technique, federated learning, has gained much traction. Instead of collecting and sending the entire data to the cloud, federated learning allows users to collaboratively train a model by only sending weight updates to a server [191]. The use of federated learning in supply chain applications needs to be explored in the future.
5) The rapid increase in the global population has brought several issues to the forefront: environmental pollution, water shortages, ecological damage, and global warming. To this end, research in the direction of green logistics and circular supply chain is much needed. Besides remanufacturing and reverse logistics, the development of green economic policies for lower carbon emissions can also become a critical field for research.

XI. Conclusion

As supply chain leaders continue their digital transformation journey, modern technologies are expected to become an inherent part of the day to day businesses, accelerating the way toward automated, proactive, predictive, and personalized future for logistics. By reviewing and analyzing the recent works in the direction of supply chain management, this article contributes to a better understanding of the present scenario of supply chain planning and management. In particular, this article addresses the various challenges and security issues in the way of efficient supply chain management, the security-critical application areas of the supply chain, as well as the various state-of-the-art technologies that have the potential to revolutionize several supply chain processes. Furthermore, this article also discusses existing and upcoming solutions to the supply chain security issues arising from the adoption of the techniques mentioned above. These solutions include—blockchain, AI, and PUFs.

References

[1] OECD/EUIPO. (2019). *Trends in Trade in Counterfeit and Pirated Goods*. [Online]. Available: https://doi.org/10.1787/g2g9f533-en
[2] L. Wainstein. (Dec. 2018). *Supply Chain Security—Cybersecurity and Supply Chain Management*. [Online]. Available: https://supplychainbeyond.com/7-supply-chain-security-concerns-to-address-in-2019/
[3] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Feb. 2020.
[4] G. Lu, X. Koufteros, and L. Lucianetti, "Supply chain security: A classification of practices and an empirical study of differential effects and complementarity," *IEEE Trans. Eng. Manag.*, vol. 64, no. 2, pp. 234–248, Feb. 2017.
[5] B. Al Sabbagh and S. Kowalski, "A socio-technical framework for threat modeling a software supply chain," *IEEE Security Privacy*, vol. 13, no. 4, pp. 30–39, Jul. 2015.
[6] S. S. Ali, M. Ibrahim, J. Rajendran, O. Sinanoglu, and K. Chakrabarty, "Supply-chain security of digital microfluidic biochips," *Computer*, vol. 49, no. 8, pp. 36–43, 2016.
[7] P. Ralston, D. Fry, S. Suko, B. Winters, M. King, and R. Kober, "Defeating counterfeiters with microscopic dielets embedded in electronic components," *Computer*, vol. 49, no. 8, pp. 18–26, 2016.
[8] J. Huang, X. Li, C.-C. Xing, W. Wang, K. Hua, and S. Guo, "DTD: A novel double-track approach to clone detection for RFID-enabled supply chains," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 1, pp. 134–140, Jan. 2015.
[9] J. P. Skudlarek, T. Katsioulas, and M. Chen, "A platform solution for secure supply-chain and chip life-cycle management," *Computer*, vol. 49, no. 8, pp. 28–34, 2016.
[10] D. Zhang, X. Wang, M. T. Rahman, and M. Tehranipoor, "An on-chip dynamically obfuscated wrapper for protecting supply chain against IP and IC piracies," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 11, pp. 2456–2469, Jul. 2018.
[11] X. Wang, D. Zhang, M. He, D. Su, and M. Tehranipoor, "Secure scan and test using obfuscation throughout supply chain," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 9, pp. 1867–1880, Nov. 2017.
[12] A. Esfahani *et al.*, "An efficient Web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain," *IEEE Access*, vol. 7, pp. 58981–58989, 2019.
[13] C. K. Wu *et al.*, "Supply chain of things: A connected solution to enhance supply chain productivity," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 78–83, Aug. 2019.
[14] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019.
[15] V. Hassija, V. Chamola, N. G. K. Dara, and M. Guizani, "A distributed framework for energy trading between UAVs and charging stations," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5391–5402, May 2020.

[16] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, Jun. 2020.

[17] V. Hassija, V. Gupta, S. Garg, and V. Chamola, "Traffic jam probability estimation based on blockchain and deep neural networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 3, 2020, doi: 10.1109/TITS.2020.2988040.

[18] V. Hassija, V. Chamola, G. Han, J. Rodrigues, and M. Guizani, "DAGIoV: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4182–4191, Apr. 2020.

[19] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, 2016, pp. 2663–2668.

[20] V. Hassija, V. Chamola, V. Gupta, and G. S. S. Chalapathi, "A framework for secure vehicular network using advanced blockchain," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, 2020, pp. 1260–1265.

[21] V. Hassija, V. Saxena, and V. Chamola, "A mobile data offloading framework based on a combination of blockchain and virtual voting," *Softw. Pract. Exp.*, to be published.

[22] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy management: Review, solutions, and challenges," *Comput. Commun.*, vol. 151, pp. 395–418, Feb. 2020.

[23] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," *Sensors*, vol. 19, no. 22, p. 4862, 2019.

[24] G. Praveen, V. Chamola, V. Hassija, and N. Kumar, "Blockchain for 5G: A prelude to future telecommunication," *IEEE Netw.*, early access, Apr. 30, 2020, doi: 10.1109/MNET.001.2000005.

[25] V. Hassija, V. Chamola, V. Gupta, and G. S. S. Chalapathi, "A blockchain based framework for secure data offloading in tactile Internet environment," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, 2020, pp. 1836–1841.

[26] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019.

[27] N. Kshetri and E. Loukoianova, "Blockchain adoption in supply chain networks in asia," *IT Prof.*, vol. 21, no. 1, pp. 11–15, 2019.

[28] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019.

[29] B. Zalud. *The Daily Challenges of Supply Chain Security*. Accessed: Apr. 1, 2016. [Online]. Available: https://www.securitymagazine.com/articles/87010-the-daily-challenges-of-supply-chain-security

[30] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Comput. Commun.*, vol. 155, pp. 1–8, Apr. 2020.

[31] R. O'Byrne, *The Changing Face of Supply Chain Security*. Accessed: Nov. 27, 2017. [Online]. Available: https://www.logisticsbureau.com/changing-face-of-supply-chain-security/

[32] G. K. Verma, B. B. Singh, N. Kumar, and V. Chamola, "CB-CAS: Certificate-based efficient signature scheme with compact aggregation for industrial Internet of Things environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2563–2572, Apr. 2020.

[33] W. Shepard. (May 2018). *Meet the Man Fighting America's Trade War Against Chinese Counterfeits (It's Not Trump)*. [Online]. Available: https://www.forbes.com/sites/wadeshepard/2018/03/29/meet-the-man-fighting-americas-trade-war-against-chinese-counterfeits

[34] R. Coates. (Feb. 2019). *Counterfeits Are Still a Major Problem*. [Online]. Available: https://www.scmr.com/article/counterfeits_are_still_a_major_problem

[35] InfoSec Institute. *Cyber Security Risk in Supply Chain Management: Part 1*. Accessed: Nov. 27, 2017. [Online]. Available: https://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/

[36] Paul Trudgian Ltd. *How Security Problems Affect the Supply Chain*. Accessed: Sep. 18, 2016. [Online]. Available: https://www.paultrudgian.co.uk/security-problems-supply-chain/

[37] P. Institute. (Nov. 2018). *Data Risk in the Third-Party Ecosystem: Third Annual Report*. [Online]. Available: https://promotions.opus.com/l/12092/2018-11-14/6bj4g6

[38] I. Ponemon. (Dec. 2018). *Measuring & Managing the Cyber Risks to Business Operations*. [Online]. Available: https://www.tenable.com/ponemon-report/cyber-risk#download

[39] T. Appleby. *Supply Chain Threats in 2019 and Beyond*. Accessed: Jul. 23, 2019. [Online]. Available: https://resources.infosecinstitute.com/supply-chain-threats/

[40] B. Thomas. (Oct. 2019). *Airbus Incident Shines Spotlight on Third-Party Vendor Security Risks*. [Online]. Available: https://www.bitsight.com/blog/airbus-incident-shines-spotlight-on-third-party-vendor-security-risks

[41] A. Madadi, M. E. Kurz, K. M. Taaffe, J. L. Sharp, and S. J. Mason, "Supply network design: Risk-averse or risk-neutral?" *Comput. Ind. Eng.*, vol. 78, pp. 55–65, Dec. 2014.

[42] S. Van Niekerk, W. Niemann, T. Kotzé, and K. Mocke, "Supply chain security orientation in the pharmaceutical industry," *Southern African Bus. Rev.*, vol. 21, no. 1, pp. 446–479, 2017.

[43] G. J. Buckley *et al.*, *Countering the Problem of Falsified and Substandard Drugs*. New York, NY, USA: Nat. Acad. Press, 2013.

[44] M. D. Voss and Z. Williams, "Public-private partnerships and supply chain security: C-TPAT as an indicator of relational security," *J. Bus. Logist.*, vol. 34, no. 4, pp. 320–334, 2013.

[45] A. Rong, R. Akkerman, and M. Grunow, "An optimization approach for managing fresh food quality throughout the supply chain," *Int. J. Prod. Econ.*, vol. 131, no. 1, pp. 421–429, 2011.

[46] Q. Tao, C. Gu, Z. Wang, J. Rocchio, W. Hu, and X. Yu, "Big data driven agricultural products supply chain management: A trustworthy scheduling optimization approach," *IEEE Access*, vol. 6, pp. 49990–50002, 2018.

[47] X. Jing, Z. Dongjie, and M. Zhongsu, "The research on the BP neural network application in food supply chain risk management," in *Proc. Int. Conf. Inf. Manag. Innov. Manag. Ind. Eng.*, vol. 1, Dec. 2009, pp. 545–548.

[48] *Your Software Supply Chain: Understanding and Optimizing for Success*. Accessed: Feb. 16, 2020. [Online]. Available: https://sentinel.gemalto.com/blog/optimizing-your-software-supply-chain/

[49] S. Uddin and A. A. A. A. Sharif, "Integrating Internet of Things with maintenance spare parts' supply chain," in *Proc. 5th Int. Conf. Electron. Devices Syst. Appl. (ICEDSA)*, Dec. 2016, pp. 1–4.

[50] D. A. Bodner, "Enterprise modeling framework for counterfeit parts in defense systems," *Procedia Comput. Sci.*, vol. 36, pp. 425–431, Jul. 2014.

[51] M. M. Tehranipoor, U. Guin, and D. Forte, "Counterfeit integrated circuits," in *Counterfeit Integrated Circuits*. Heidelberg, Germany: Springer, 2015, pp. 15–36.

[52] J. Arora. *Securing the Supply Chain Is as Important as Securing the Front Door*. Accessed: Sep. 25, 2017. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/securing-the-supply-chain-is-as-important-as-securing-the-front-door

[53] (Jan. 2018). *Top 5 Challenges in the Retail Supply Chain*. [Online]. Available: https://www.spendedge.com/blogs/top-challenges-retail-supply-chain

[54] *Short-Term Energy Outlook (STEO)*. U.S. Energy Inf. Admin., Washington, DC, USA, Mar. 2020. [Online]. Available: https://www.eia.gov/outlooks/steo/pdf/steo_full.pdf

[55] P. Hobson. (Aug. 2019). *Fake-Branded Bars Slip Dirty Gold Into World Markets*. [Online]. Available: https://www.reuters.com/article/us-gold-swiss-fakes-exclusive/exclusive-fake-branded-bars-slip-dirty-gold-into-world-markets-idUSKCN1VI0DD

[56] P. Kittipanya-ngam and K. H. Tan, "A framework for food supply chain digitalization: Lessons from thailand," *Prod. Plan. Control*, vol. 31, nos. 2–3, pp. 158–172, 2020.

[57] C. Klötzer and A. Pflaum, "Toward the development of a maturity model for digitalization within the manufacturing industry's supply chain," in *Proc. Hawaii Int. Conf. Syst. Sci.*, Waikoloa Village, HI, USA, 2017.

[58] D. C. Feibert, M. S. Hansen, and P. Jacobsen, "An integrated process and digitalization perspective on the shipping supply chain—A literature review," in *Proc. IEEE Int. Conf. Ind. Eng. Manag. (IEEM)*, 2017, pp. 1352–1356.

[59] A. Genovese, A. A. Acquaye, A. Figueroa, and S. L. Koh, "Sustainable supply chain management and the transition towards a circular economy: Evidence and some applications," *Omega*, vol. 66, pp. 344–357, Jan. 2017.

[60] M. Geissdoerfer, S. N. Morioka, M. M. de Carvalho, and S. Evans, "Business models and supply chains for the circular economy," *J. Clean. Prod.*, vol. 190, pp. 712–721, Jul. 2018.

[61] R. D. Angelis, M. Howard, and J. Miemczyk, "Supply chain management and the circular economy: Towards the circular supply chain," *Prod. Plan. Control*, vol. 29, no. 6, pp. 425–437, 2018.

[62] M. N. Shafique, M. M. Khurshid, H. Rahman, A. Khanna, D. Gupta, and J. J. P. C. Rodrigues, "The role of wearable technologies in supply chain collaboration: A case of pharmaceutical industry," *IEEE Access*, vol. 7, pp. 49014–49026, 2019.

[63] A. Robinson. (Mar. 2016). *Wearable Technology in the Supply Chain: 3 Benefits*. [Online]. Available: https://cerasis.com/wearable-technology-in-the-supply-chain/

[64] K. Herhold. (Jan. 2020). *Three Ways Wearables Boost Supply-Chain Efficiency*. [Online]. Available: https://www.supplychainbrain.com/blogs/1-think-tank/post/30765-three-ways-that-wearables-increase-supply-chain-efficiency

[65] C. G. Cegielski, L. A. Jones-Farmer, Y. Wu, and B. T. Hazen, "Adoption of cloud computing technologies in supply chains," *Int. J. Logist. Manag.*, vol. 23, no. 2, pp. 184–211, 2012.

[66] Y. Wu, C. G. Cegielski, B. T. Hazen, and D. J. Hall, "Cloud computing in support of supply chain information system infrastructure: Understanding when to go to the cloud," *J. Supply Chain Manag.*, vol. 49, no. 3, pp. 25–41, 2013.

[67] Q. Cao, D. G. Schniederjans, and M. Schniederjans, "Establishing the use of cloud computing in supply chain management," *Oper. Manag. Res.*, vol. 10, nos. 1–2, pp. 47–63, 2017.

[68] S. Tiwari, H. M. Wee, and Y. Daryanto, "Big data analytics in supply chain management between 2010 and 2016: Insights to industries," *Comput. Ind. Eng.*, vol. 115, pp. 319–330, Nov. 2018.

[69] A. Gunasekaran *et al.*, "Big data and predictive analytics for supply chain and organizational performance," *J. Bus. Res.*, vol. 70, pp. 308–317, Sep. 2017.

[70] T. Nguyen, Z. Li, V. Spiegler, P. Ieromonachou, and Y. Lin, "Big data analytics in supply chain management: A state-of-the-art literature review," *Comput. Oper. Res.*, vol. 98, pp. 254–264, Sep. 2018.

[71] X. J. Fu *et al.*, "Social media for supply chain risk management," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag.*, 2013, pp. 206–210.

[72] A. Singh, N. Shukla, and N. Mishra, "Social media data analytics to improve supply chain management in food industries," *Transp. Res. E Logist. Transport. Rev.*, vol. 114, no. 1, pp. 398–415, 2018.

[73] D. E. O'leary, "The use of social media in the supply chain: Survey and extensions," *Intell. Syst. Accounting Finance Manag.*, vol. 18, nos. 2–3, pp. 121–144, 2011.

[74] K. Alicke, J. Rachor, and A. Seyfert. (Oct. 2016). *Supply Chain 4.0—The Next-Generation Digital Supply Chain*. [Online]. Available: https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-40–the-next-generation-digital-supply-chain

[75] MHI. (2020). *The 2020 MHI Annual Industry Report—Embracing the Digital Mindset Deloitte*. [Online]. Available: https://www.mhi.org/publications/report

[76] A&A. *Top 10 Future Trends in Supply Chain and Logistics*. [Online]. Available: https://aacb.com/trends-in-supply-chain-and-logistics/

[77] M. Farooque, A. Zhang, M. Thurer, T. Qu, and D. Huisingh, "Circular supply chain management: A definition and structured literature review," *J. Clean. Prod.*, vol. 228, pp. 882–900, Aug. 2019.

[78] P. V. D. Bossche, C. Simpson, D. Weiser, and N. Anderson. (Feb. 2016). *Wearable Technology in the Warehouse—Supply Chain 24/7*. [Online]. Available: https://www.supplychain247.com/article/wearable_technology_in_the_warehouse

[79] K. Alicke, C. Glatzel, P.-M. Karlsson, and K. Hoberg. (2016). *Big Data and the Supply Chain: The Big-Supply-Chain Analytics Landscape (Part 1)*. [Online]. Available: https://www.mckinsey.com/business-functions/operations/our-insights/big-data-and-the-supply-chain-the-big-supply-chain-analytics-landscape-part-1

[80] R. Sinha. (Jan. 2019). *Role of Social Media in Supply Chain Management*. [Online]. Available: https://medium.com/boardinfinity/role-of-social-media-in-supply-chain-management-f4ebc92099ea

[81] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *IEEE Access*, vol. 8, pp. 90225–90265, 2020.

[82] D. Kaid and M. M. Eljazzar, "Applying blockchain to automate installments payment between supply chain parties," in *Proc. 14th Int. Comput. Eng. Conf. (ICENCO)*, Dec. 2018, pp. 231–235.

[83] A. E. C. Mondragon, C. E. Coronado, and E. S. Coronado, "Investigating the applicability of distributed ledger/blockchain technology in manufacturing and perishable goods supply chains," in *Proc. IEEE 6th Int. Conf. Ind. Eng. Appl. (ICIEA)*, Apr. 2019, pp. 728–732.

[84] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 568–570.

[85] N. Saxena, I. Thomas, P. Gope, P. Burnap, and N. Kumar, "PharmaCrypt: Blockchain for critical pharmaceutical industry to counterfeit drugs," *Computer*, vol. 53, no. 7, pp. 29–44, 2020.

[86] A. Kumar, D. Choudhary, M. S. Raju, D. K. Chaudhary, and R. K. Sagar, "Combating counterfeit drugs: A quantitative analysis on cracking down the fake drug industry by using blockchain technology," in *Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. (Confluence)*, Jan. 2019, pp. 174–178.

[87] R. Jayaraman, F. AlHammadi, and M. C. E. Simsekler, "Managing product recalls in healthcare supply chain," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag. (IEEM)*, Dec. 2018, pp. 293–297.

[88] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, May 2017, pp. 772–777.

[89] R. C. Celiz, Y. E. De La Cruz, and D. M. Sanchez, "Cloud model for purchase management in health sector of Peru based on IoT and blockchain," in *Proc. IEEE 9th Annu. Inf. Technol. Electron. Mobile Commun. Conf. (IEMCON)*, Nov 2018, pp. 328–334.

[90] J. Hua, X. Wang, M. Kang, H. Wang, and F. Wang, "Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping," in *Proc. IEEE Intell. Veh. Symp. (IV)*, Jun. 2018, pp. 97–101.

[91] Y. Fu and J. Zhu, "Big production enterprise supply chain endogenous risk management based on blockchain," *IEEE Access*, vol. 7, pp. 15310–15319, 2019.

[92] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018.

[93] H. Pervez and I. U. Haq, "Blockchain and IoT based disruption in logistics," in *Proc. 2nd Int. Conf. Commun. Comput. Digit. Syst. (C-CODE)*, Mar. 2019, pp. 276–281.

[94] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag. (IEEM)*, Dec. 2017, pp. 1357–1361.

[95] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manag.*, Jun. 2017, pp. 1–6.

[96] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. IEEE 13th Int. Conf. Service Syst. Service Manag. (ICSSSM)*, 2016, pp. 1–6.

[97] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5803–5813, Jun. 2019.

[98] M. Kim, B. Hilton, Z. Burks, and J. Reyes, "Integrating blockchain, smart contract-tokens, and IoT to design a food traceability solution," in *Proc. IEEE 9th Annu. Inf. Technol. Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2018, pp. 335–340.

[99] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in *Proc. IoT Vertical Topical Summit Agricult. Tuscany (IOT Tuscany)*, May 2018, pp. 1–4.

[100] G. R. Chandra, I. A. Liaqat, and B. Sharma, "Blockchain redefining: The halal food sector," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 349–354.

[101] C.-C. Lin, S.-C. Shieh, Y.-H. Kao, Y.-T. Chang, and S.-S. Chen, "The simulation analysis of push and pull shelf replenishment policies for retail supply chain," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 7, Jul. 2008, pp. 3964–3969.

[102] F. De Sousa Ribeiro, F. Caliva, M. Swainson, K. Gudmundsson, G. Leontidis, and S. Kollias, "An adaptable deep learning system for optical character verification in retail food packaging," in *Proc. IEEE Conf. Evol. Adapt. Intell. Syst. (EAIS)*, May 2018, pp. 1–8.

[103] X. Bao, Q. Lu, S. Wu, and Y. Wang, "Application of MID-based RFID handset in food traceability," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 1, Jul. 2011, pp. 410–413.

[104] M. Alsallal, M. S. Sharif, B. Al-Ghzawi, and S. M. M. A. Mutoki, "A machine learning technique to detect counterfeit medicine based on X-Ray fluorescence analyser," in *Proc. Int. Conf. Comput. Electron. Commun. Eng. (iCCECE)*, Aug 2018, pp. 118–122.

[105] C. Yang, "Collaborative mechanism of manufacturing enterprise supply chain based on multi-agent," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 1, Aug. 2007, pp. 198–201.

[106] X.-L. Tang, "Study on selection of logistics supplier based on support vector machine," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 2, Jul. 2009, pp. 1231–1235.

[107] X.-B. Liu, H.-G. Bo, Y. Ma, and Q.-N. Meng, "Study on supply chain-oriented hybrid planning and scheduling system for iron and steel enterprises," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 2, Aug. 2005, pp. 993–997.

[108] S. Dong, L. Tian, and R. Li, "Separating equilibrium of ordering process in supply chain under the presence of demand information leakage," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 3, Jul. 2011, pp. 1037–1042.

[109] G.-X. Liu and F. Liu, "IoT-based TPL whole supply chain logistics information system model," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 4, Jul. 2013, pp. 1758–1762.

[110] H. Xue, C. Jiang, B. Cai, and Y. Yuan, "Research on demand forecasting of retail supply chain emergency logistics based on NRS-GA-SVM," in *Proc. Chin. Control Decis. Conf. (CCDC)*, Jun. 2018, pp. 3647–3652.

[111] J. Wu, A. Olesnikova, C. Song, and W. D. Lee, "The development and application of decision tree for agriculture data," in *Proc. 2nd Int. Symp. Intell. Inf. Technol. Security Informat.*, Jan. 2009, pp. 16–20.

[112] L. Huang, "Recognizing real customers in e-supply chain based on SOFM neural network and corresponding marketing strategies," in *Proc. Int. Conf. Mach. Learn. Cybern.*, Aug. 2006, pp. 1592–1597.

[113] M. Takahashi, M. Nagata, and N. Miura, "Supply-chain security enhancement by chaotic wireless chip-package-board interactive PUF," in *Proc. IEEE 68th Electron. Compon. Technol. Conf. (ECTC)*, May 2018, pp. 521–526.

[114] P. F. Cortese, F. Gemmiti, B. Palazzi, M. Pizzonia, and M. Rimondini, "Efficient and practical authentication of PUF-based RFID tags in supply chains," in *Proc. IEEE Int. Conf. RFID Technol. Appl.*, Jun. 2010, pp. 182–188.

[115] N. Miura, M. Takahashi, K. Nagatomo, and M. Nagata, "Chaos, deterministic non-periodic flow, for chip-package-board interactive PUF," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2017, pp. 25–28.

[116] B. Ray, M. Chowdhury, and J. Abawaiy, "PUF-based secure checker protocol for networked RFID systems," in *Proc. IEEE Conf. Open Syst. (ICOS)*, Oct. 2014, pp. 78–83.

[117] N. Miura, M. Takahashi, K. Nagatomo, and M. Nagata, "Chip-package-board interactive PUF utilizing coupled chaos oscillators with inductor," *IEEE J. Solid-State Circuits*, vol. 53, no. 10, pp. 2889–2897, Oct. 2018.

[118] Q. Li, X. Xu, and Z. Chen, "PUF-based RFID ownership transfer protocol in an open environment," in *Proc. 15th Int. Conf. Parallel Distrib. Comput. Appl. Technol.*, Dec. 2014, pp. 131–137.

[119] M. Uddin, M. B. Majumder, and G. S. Rose, "Robustness analysis of a memristive crossbar PUF against modeling attacks," *IEEE Trans. Nanotechnol.*, vol. 16, no. 3, pp. 396–405, May 2017.

[120] S. B. Dodo, R. Bishnoi, S. M. Nair, and M. B. Tahoori, "A spintronics memory PUF for resilience against cloning counterfeit," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 11, pp. 2511–2522, Nov. 2019.

[121] V. Rožić, B. Yang, J. Vliegen, N. Mentens, and I. Verbauwhede, "The Monte Carlo PUF," in *Proc. 27th Int. Conf. Field Program. Logic Appl. (FPL)*, Sep. 2017, pp. 1–6.

[122] P. Prabhu *et al.*, "Extracting device fingerprints from flash memory by exploiting physical variations," in *Proc. Int. Conf. Trust Trustworthy Comput.*, 2011, pp. 188–201.

[123] L. Aniello, B. Halak, P. Chai, R. Dhall, M. Mihalea, and A. Wilczynski, "Towards a supply chain management system for counterfeit mitigation using blockchain and PUF," 2019. [Online]. Available: arXiv:1908.09585.

[124] Y. Yilmaz, S. R. Gunn, and B. Halak, "Lightweight PUF-based authentication protocol for IoT devices," in *Proc. IEEE 3rd Int. Verification Security Workshop (IVSW)*, 2018, pp. 38–43.

[125] U. Chatterjee *et al.*, "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database," *IEEE Trans. Depend. Secure Comput.*, vol. 16, no. 3, pp. 424–437, May 2018.

[126] A. Wild, G. T. Becker, and T. Güneysu, "A fair and comprehensive large-scale analysis of oscillation-based PUFs for FPGAs," in *Proc. IEEE 27th Int. Conf. Field Program. Logic Appl. (FPL)*, 2017, pp. 1–7.

[127] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, 2007, pp. 9–14.

[128] P. Tuyls and B. Škorić, *Strong Authentication With Physical Unclonable Functions*. Berlin, Germany: Springer, 2007, pp. 133–148. [Online]. Available: https://doi.org/10.1007/978-3-540-69861-6_10

[129] W. Che, F. Saqib, and J. Plusquellic, "PUF-based authentication," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, 2015, pp. 337–344.

[130] J. Delvaux, R. Peeters, D. Gu, and I. Verbauwhede, "A survey on lightweight entity authentication with strong PUFs," *ACM Comput. Surveys*, vol. 48, no. 2, p. 26, Oct. 2015. [Online]. Available: https://doi.org/10.1145/2818186

[131] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, "Secure lightweight entity authentication with strong PUFs: Mission impossible?" in *Cryptographic Hardware and Embedded Systems—CHES 2014*, L. Batina and M. Robshaw, Eds. Berlin, Germany: Springer, 2014, pp. 451–475.

[132] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for rfid systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.

[133] P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, "A secure iot-based modern healthcare system with fault-tolerant decision making process," *IEEE J. Biomed. Health Inform.*, early access, Jul. 7, 2020, doi: 10.1109/JBHI.2020.3007488.

[134] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of drones," *IEEE Trans. Veh. Technol.*, early access, Aug. 24, 2020, doi: 10.1109/TVT.2020.3018778.

[135] P. Koeberl, J. Li, A. Rajan, C. Vishik, and W. Wu, "A practical device authentication scheme using SRAM PUFs," in *Trust and Trustworthy Computing*, J. M. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, A. Sasse, and Y. Beres, Eds. Berlin, Germany: Springer, 2011, pp. 63–77.

[136] M. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, "A lockdown technique to prevent machine learning on PUFs for lightweight authentication," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 3, pp. 146–159, Apr. 2016.

[137] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based 'Unclonable' RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 58–64.

[138] C. Hristea and F. L. Ţiplea, "A PUF-based destructive private mutual authentication RFID protocol," in *Innovative Security Solutions for Information Technology and Communications*, J.-L. Lanet and C. Toma, Eds. Cham, Switzerland: Springer Int., 2019, pp. 331–343.

[139] H.-H. Huang, L.-Y. Yeh, and W.-J. Tsaur, "PUF-based protocols about mutual authentication and ownership transfer for RFID Gen2 V2 systems," in *Transactions on Engineering Technologies*, S.-I. Ao, H. K. Kim, X. Huang, and O. Castillo, Eds. Singapore: Springer, 2017, pp. 49–59.

[140] M. N. Islam and S. Kundu, "Enabling IC traceability via blockchain pegged to embedded PUF," *ACM Trans. Design Autom. Electron. Syst.*, vol. 24, no. 3, p. 36, Apr. 2019. [Online]. Available: https://doi.org/10.1145/3315669

[141] N. Garrett. (Oct. 2019). *Blockchain Helps Trace Responsibly Produced Raw Materials*. [Online]. Available: https://www.ibm.com/blogs/blockchain/2019/10/blockchain-helps-trace-responsibly-produced-raw-materials/

[142] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[143] L. Pawczuk, J. Holdowsky, R. Massey, and B. Hansen, *Thriving in the Era of Pervasive AI*. Deloitte, London, U.K., 2020. [Online]. Available: https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf

[144] G. Samman. (May 2016). *'Immutable Me' a Discussion Paper Exploring Data Provenance to Enable New Value Chains*. [Online]. Available: http://sammantics.com/blog/2016/5/18/immutable-me-a-discussion-paper-exploring-data-provenance-to-enable-new-value-chains

[145] R. Mitra. (2019). *Blockchain and Supply Chain: A Dynamic Duo*. [Online]. Available: https://blockgeeks.com/guides/blockchain-and-supply-chain/

[146] R. O'Byrne. (Jan. 2019). *Blockchain Technology Is Set to Transform the Supply Chain*. [Online]. Available: https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/

[147] Hyperledger. (Feb. 2019). *How Walmart Brought Unprecedented Transparency to the Food Supply Chain With Hyperledger Fabric*. Accessed: Jul. 14, 2020. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf

[148] J. Keil. (Nov. 2019). *Blockchain in Supply Chain Management: Key Use Cases and Benefits*. [Online]. Available: https://www.infopulse.com/blog/blockchain-in-supply-chain-management-key-use-cases-and-benefits/

[149] M. Pratap. (Aug. 2018). *How Is Blockchain Disrupting the Supply Chain Industry?* [Online]. Available: https://hackernoon.com/how-is-blockchain-disrupting-the-supply-chain-industry-f3a1c599daef

[150] *About Tradelens*. Accessed: Jul. 14, 2020. [Online]. Available: https://www.tradelens.com/about

[151] G. Prause, "Smart contracts for smart supply chains," *IFAC PapersOnLine*, vol. 52, no. 13, pp. 2501–2506, 2019.

[152] A. Law, "Smart contracts and their application in supply chain management," Ph.D. dissertation, Dept. Comput. Eng., Massachusetts Inst. Technol., Cambridge, MA, USA, 2017.

[153] *Smart Contracts*. Accessed: Jun. 15, 2020. [Online]. Available: https://www.adaptideations.com/smart-contracts

[154] S. Perrenod and S. Khan. (May 2020). *Blockchain: Streamlining Disrupted Supply Chains During Covid Crisis*. [Online]. Available: https://www.enterpriseai.news/2020/05/07/blockchain-streamlining-disrupted-supply-chains-during-covid-crisis/

[155] A. Takyar. (Mar. 2020). *Food Supply Chain Blockchain—Solving Food Supply Problems*. [Online]. Available: https://www.leewayhertz.com/supply-chain-blockchain-reinventing-food-supply/

[156] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "BlockCom: A blockchain based commerce model for smart communities using auction mechanism," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[157] D. Khasis. (Aug. 2019). *Four Ways AI Is Impacting Logistics and Supply Chain Management*. [Online]. Available: https://www.supplychainbrain.com/blogs/1-think-tank/post/30045-four-ways-ai-is-impacting-logistics-and-supply-chain-management

[158] A. Cam, M. Chui, and B. Hall. (Nov. 2019). *Global AI Survey: AI Proves Its Worth, But Few Scale Impact*. [Online]. Available: https://www.mckinsey.com/featured-insights/artificial-intelligence/global-ai-survey-ai-proves-its-worth-but-few-scale-impact

[159] C. Pettey. (Apr. 2019). *Gartner Top 8 Supply Chain Technology Trends for 2019*. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-8-supply-chain-technology-trends-for-2019/

[160] H. Oti-Yeboah. (Sep. 2018). *Why Is Demand Forecasting Important for Effective Supply Chain Management? Supply Chain Link Blog*. [Online]. Available: https://blog.arkieva.com/demand-forecasting-for-supply-chain-management/

[161] L. A. Deleris and F. Erhun, *Quantitative Risk Assessment in Supply Chains: A Case Study Based on Engineering Risk Analysis Concepts*. New York, NY, USA: Springer, 2011, pp. 105–131. [Online]. Available: https://doi.org/10.1007/978-1-4419–8191-2_5

[162] E. M. Goldratt and J. Cox, *The Goal: A Process of Ongoing Improvement*. London, U.K.: Routledge, 2016.

[163] K. R. Community and S. Jenks. (Oct. 2017). *6 Applications of Artificial Intelligence for Your Supply Chain*. [Online]. Available: https://medium.com/@KodiakRating/6-applications-of-artificial-intelligence-for-your-supply-chain-b82e1e7400c8

[164] (Sep. 2017). *Supply Chain Losing Hours, Money to Poor Financial Systems*. [Online]. Available: https://www.mhlnews.com/global-supply-chain/article/22054569/supply-chain-losing-hours-money-to-poor-financial-systems

[165] B. Ammanath, D. Jarvis, and S. Hupfer. (Jul. 2020). *Thriving in the Era of Pervasive AI*. [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/state-of-ai-and-intelligent-automation-in-business-survey.html

[166] Accenture Interactive. (2016). *Chatbots in Customer Support*. [Online]. Available: https://www.accenture.com/t00010101T000000__w__/br-pt/_acnmedia/PDF-45/Accenture-Chatbots-Customer-Service.pdf

[167] A. Enterprise. (Jul. 2019). *The Rise of Chatbots in Supply Management and Why You Should Care*. [Online]. Available: https://chatbotslife.com/the-rise-of-chatbots-in-supply-management-and-why-you-should-care-fcd0d9506a0

[168] G. Baryannis, S. Dani, and G. Antoniou, "Predicting supply chain risks using machine learning: The trade-off between performance and interpretability," *Future Gener. Comput. Syst.*, vol. 101, pp. 993–1004, Dec. 2019.

[169] E. Camossi, T. Dimitrova, and A. Tsois, "Detecting anomalous maritime container itineraries for anti-fraud and supply chain security," in *Proc. Eur. Intell. Security Informat. Conf.*, Aug. 2012, pp. 76–83.

[170] A. Allgurin and F. Karlsson, *Exploring Machine Learning for Supplier Selection: A Case Study at BUFAB Sweden AB*, Linnaeus Univ., Växjö, Sweden, 2018.

[171] M. J. Nodeh, M. H. Calp, and İ. Şahin, "A novel hybrid model for vendor selection in a supply chain by using artificial intelligence techniques case study: Petroleum companies," in *Proc. Int. Conf. Artif. Intell. Appl. Math. Eng.*, 2019, pp. 226–251.

[172] T. Alladi, N. Naren, and V. Chamola, "HARCI: A two-way authentication protocol for three entity healthcare IoT networks," *IEEE J. Sel. Areas Commun.*, early access, Sep. 1, 2020, doi: 10.1109/JSAC.2020.3020605.

[173] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[174] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7234–7246, Jul. 2020.

[175] T. Bauer and J. Hamlet, "Physical unclonable functions: A primer," *IEEE Security Privacy*, vol. 12, no. 6, pp. 97–101, Nov./Dec. 2014.

[176] G. Kulkarni, R. Shelke, R. Sutar, and S. Mohite, "RFID security issues & challenges," in *Proc. Int. Conf. Electron. Commun. Syst. (ICECS)*, 2014, pp. 1–4.

[177] M. El Beqqal and M. Azizi, "Review on security issues in RFID systems," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 2, no. 6, pp. 194–202, 2017.

[178] S. Devadas, "Non-networked RFID-PUF authentication," U.S. Patent 8 683 210, Mar. 2014.

[179] B. Marr. (Dec. 2019). *What Is the Artificial Intelligence of Things? When AI Meets IoT*. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2019/12/20/what-is-the-artificial-intelligence-of-things-when-ai-meets-iot/#5febae9eb1fd

[180] Z. Gao, C. Xu, H. Zhang, S. Li, and V. H. C. de Albuquerque, "Trustful Internet of surveillance things based on deeply represented visual co-saliency detection," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4092–4100, Jan. 2020.

[181] M. A. Santos, R. Munoz, R. Olivares, P. P. R. Filho, J. D. Ser, and V. H. C. de Albuquerque, "Online heart monitoring systems on the Internet of Health Things environments: A survey, a reference model and an outlook," *Inf. Fusion*, vol. 53, pp. 222–239, Jan. 2020.

[182] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, 2019.

[183] L. Oliveira, J. J. Rodrigues, S. A. Kozlov, R. A. Rabêlo, and V. H. C. D. Albuquerque, "MAC layer protocols for Internet of Things: A survey," *Future Internet*, vol. 11, no. 1, p. 16, 2019.

[184] S. Pirbhulal, W. Wu, K. Muhammad, I. Mehmood, G. Li, and V. H. C. de Albuquerque, "Mobility enabled security for optimizing IoT based intelligent applications," *IEEE Netw.*, vol. 34, no. 2, pp. 72–77, Apr. 2020.

[185] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, pp. 147–157, Mar. 2019.

[186] M. A. A. da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. de Albuquerque, "A reference model for Internet of Things middleware," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 871–883, Apr. 2018.

[187] R. R. Guimaraes *et al.*, "Intelligent network security monitoring based on optimum-path forest clustering," *IEEE Netw.*, vol. 33, no. 2, pp. 126–131, Mar./Apr. 2019.

[188] B. Cao *et al.*, "Multiobjective 3-D topology optimization of next-generation wireless data center network," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3597–3605, May 2020.

[189] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Jul. 2014.

[190] B. Halak, M. Zwolinski, and M. S. Mispan, "Overview of PUF-based hardware security solutions for the Internet of Things," in *Proc. IEEE 59th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, 2016, pp. 1–4.

[191] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

Vikas Hassija received the B.Tech. degree from Maharshi Dayanand University, Rohtak, India, in 2010, and the M.S. degree in telecommunications and software engineering from the Birla Institute of Technology and Science, Pilani, India, in 2014. He is currently pursuing the Ph.D. degree in IoT security and blockchain with the Jaypee Institute of Information and Technology (JIIT), Noida, India.

He is currently an Assistant Professor with JIIT. His research interests include the IoT security, network security, blockchain, and distributed computing.

Vinay Chamola (Senior Member, IEEE) received the B.E. degree in electrical and electronics engineering and the master's degree in communication engineering from the Birla Institute of Technology and Science (BITS), Pilani, India, in 2010 and 2013, respectively, and the Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2016.

In 2015, he was a Visiting Researcher with the Autonomous Networks Research Group, University of Southern California, Los Angeles, CA, USA. He also worked as a Postdoctoral Research Fellow with the National University of Singapore, where he worked in the area of Internet of Things. He is currently an Assistant Professor with the Department of Electrical and Electronics Engineering, BITS-Pilani, where he heads the Internet of Things Research Group/Laboratory. He has over 50 publications in high ranked SCI journals, including more than 25 IEEE TRANSACTION and journal articles. His works have been published in journals, such as IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, and *IEEE Communications Magazine*. Furthermore, his works have been accepted and presented in reputed conferences, such as IEEE INFOCOM, IEEE GLOBECOM, IEEE ICC, and IEEE PerCom to name a few. His research interests include IoT security, blockchain, 5G network management, and addressing research issues in VANETs and UAV networks.

Dr. Chamola is an Associate Editor of *Ad Hoc Networks* and *IET Quantum Communications* (Elsevier). He is also a Guest Editor of *Computer Communication* (Elsevier). He serves as a reviewer for several IEEE/Elsevier journals.

Vatsal Gupta is currently pursuing the B.Tech. degree from the Jaypee Institute of Information Technology, Noida, India.

He has completed a few projects in the field of blockchain applications, machine learning, and data analytics. He is currently (the summer of 2020) pursuing his research internship with the Birla Institute of Technology and Science Pilani, Pilani, under Dr. V. Chamola. His research interests include DLT, machine learning, and deep learning.

Sarthak Jain is currently pursuing the B.Tech. degree from the Jaypee Institute of Information Technology, Noida, India.

He has completed a few projects in the field of machine learning, natural language processing, deep learning, data science, and app development. His research interests include machine learning, deep learning, and artificial intelligence.

Nadra Guizani received the Ph.D. degree with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA, in 2020.

She is a Clinical Assistant Professor with the School of Electrical and Computer Science, Washington State University, Pullman, WA, USA. Her Ph.D. research revolved around prediction and access control of disease spread data on dynamic network topologies. Her research interests include machine learning, mobile networking, large data analysis, and prediction techniques.

Dr. Guizani is an Active Member of the Women in Engineering Program and the Computing Research Association.