„Central European Management Journal"
Vol. 29, No. 4/2021, p. 149–171, ISSN: 2658-0845, e-ISSN: 2658-2430

Analysis of Security Criteria for IoT-Based Supply Chain: A Case Study of FMCG Industries

Hamed Nozari[1], Mohammad Fallah[2], Agnieszka Szmelter-Jarosz[3], Maciej Krzemiński[4]

Submitted: 8.10.2020. Final acceptance: 16.10.2021

Abstract

Purpose: In supply chains, creating a secure space for data production, sending, storing, and analysis has always been a critical issue. The main goal of this research was to evaluate the importance of various security criteria in an intelligent supply chain system.

Methodology: The main data collection method was the expert survey. Experts validated the security criteria and sub-criteria. Then, the importance of these criteria was evaluated using the fuzzy analytic hierarchy process method.

Findings: The results revealed that reliability and privacy with their sub-criteria were the most important ones among the obtained security criteria for IoT-based supply chain management.

Practical implications: The research results can provide valuable insight for supply chains' decision--makers. The findings can also be a good reference point for researchers who work on the IoT-based supply chain concept in other countries and sectors.

Research limitations: Limitations of this study are the purposive sampling method and the limited scope of studied companies and sectors. Therefore, the article provides initial insight on the matter.

Originality: The study presents the research problem from a new perspective and gives possible solutions for IoT-based supply chain management.

Keywords: Internet of Things, Fuzzy AHP, MCDM, supply chain management, FMCG.

JEL: M15, R41

[1] Islamic Azad University – Department of Industrial Engineering of Central Tehran Branch, No. 223, Headquarter of Islamic Azad University, South Tehran Branch, ZIP area 11, Azarshahr Street, North Iranshahr Street, Karimkhan-e-Zand Avenue, Tehran, Iran; e-mail: ham.nozari.eng@iauctb.ac.ir.

[2] Islamic Azad University – Department of Industrial Engineering of Central Tehran Branch, No. 223, Headquarter of Islamic Azad University, South Tehran Branch, ZIP area 11, Azarshahr Street, North Iranshahr Street, Karimkhan-e-Zand Avenue, Tehran, Iran; e-mail: mohammad.fallah43@yahoo.com.

[3] Corresponding author: University of Gdańsk, Faculty of Economics, University of Gdańsk, ul. Armii Krajowej 119/121, 81-824 Sopot, Poland; e-mail: agnieszka.szmelter-jarosz@ug.edu.pl; https://orcid.org/0000-0002-6183-6114.

[4] University of Gdańsk, Faculty of Economics, University of Gdańsk, ul. Armii Krajowej 119/121, 81-824 Sopot, Poland; e-mail: maciej.krzeminski@ug.edu.pl.

DOI: 10.7206/cemj.2658-0845.63

Introduction

New information sources always provide opportunities for new applications to improve the quality of life and industrial activities. An enormous technological shift is expected to occur with the integration of information and communication technology and systems with areas relevant to human life, including social and economic aspects. The Internet of Things (IoT) is leading to a complete shift in environmental and urban technology in terms of complexity and diversity (Bibri, 2018). Besides, big data has been a critical factor in the realization of new IoT applications. Generally, the IoT deployment – as a computing paradigm and analytical process for big data – promotes sustainable smart initiatives and applications in the environmental and technological fields of advanced countries (Bibri and Krogstie, 2017). Despite increasing research on the IoT, much of the work primarily aims at economic growth and the quality of life in smart cities (Zanella et al., 2014). However, the IoT recently becomes increasingly intertwined with most industrial processes as support in business growth. The upply chain is one of the essential pillars of manufacturing organizations as it regulates the relationship between different sectors. All processes related to supply, production, and distribution fall into the area of the supply chain. Extensive communication with diverse individuals and units inside and outside the organization brings value to supply chain management (Dobroszek and Szychta, 2015). When the IoT relates to the supply chain, it becomes a set of physical objects connected digitally for monitoring and interaction within an enterprise that leads to data sharing, but also control and coordination of processes in the global supply chain network. Indeed, the IoT can provide new levels of supply chain visibility, agility, and adaptability to cope with various supply chain challenges (Ellis et al., 2015). Therefore, many new opportunities in applying the IoT to supply chain management can be foreseen. The number of devices connected to the Internet was expected to skyrocket and reach 50 billion by 2020 (Schliwa et al., 2015). Thus, the role of the IoT in supply chain intelligence seems crucial as the management of produced data becomes increasingly complicated, along with creating a secure space for data production, sending, storing, and analysis.

Accordingly, this study focuses on IoT-based supply chain security criteria by investigating supply chain systems of 10 selected companies from the FMCG industry. The literature review provided the potentially most critical security criteria in the IoT supply chain. The impacts of IoT on supply chain management were noticed in various processes. However, there remain issues to be tackled in IoT applications for supply chain management, specifically security. Therefore, this study seeks to evaluate supply chain management security criteria – including IoT technologies – by investigating supply chain systems of 10 companies from the FMCG industry. The main research question of our study was: What supply chain management security criteria are of the greatest importance in the FMCG supply chains based on the IoT?

The selected companies have their own supply and distribution systems due to the nature of their products, which can be perishable. Different relationships with suppliers, storage and warehousing, moving goods, communication with distributors and sellers – in addition to mass communication with consumers – are parts of the enormous data exchanged in their supply chains. Therefore, the main goal of this article is to evaluate the importance of various security criteria in a smart supply chain system, derived from a literature review and experts' opinions, along with mathematical modeling based on the method of analytic hierarchy process (AHP). This study seeks to introduce and apply fuzzy nonlinear mathematical modeling to rank security criteria of smart supply chain management (SSCM). The result of our research shows which of the potential threats to the IoT-based supply chain are the most dangerous – in the opinion of experts and practitioners who use this type of solution – which can help companies to design more secure IoT-based supply chains.

The rest of the article is organized as follows. Section 2 will present a review of the literature in terms of IoT and smart supply chains. Section 3 will present the smart supply chain security criteria. Section 4 will illustrate the mathematical modeling to analyze the criteria. The obtained findings will be presented in section 5, and finally, the discussion and conclusions will be included in Section 6.

Literature Review

The effect of the Internet of Things on various supply chain management processes, including procurement, production, distribution, reverse flow, and relevant security issues remain unknown. Therefore, we will describe the IoT concept and its effect on the supply chain management in the literature review below.

The Internet of Things

The term "Internet of Things" (IoT) was coined in the late 1990s by Kevin Ashton, the cofounder of Auto-ID Center at the Massachusetts Institute of Technology in order to examine work concerning radio-frequency identification (RFID) infrastructure (Sarma et al., 2000; Greengard, 2016). As Ashton indicates (2009), the IoT alters the equation from human-based data input to both human-based and machine-based data input, thus allowing humans and machines to gain broader and deeper insights. In fact, the

IoT not only tracks objects and collects new data but also combines them to generate a higher level of information (Greengard, 2016). The IoT was developed to describe a universal network of infrastructure in which things, wireless transmissions, and computing capabilities are combined to form a network of information (Atzori et al., 2010), creating new channels of communication and interaction with the internal and external environment (Vongsingthong and Smanchat, 2014). The Internet of Things can be applied in a vast range of application scenarios, spanning from logistics through e-health to security (Li, 2011). Some instances of physical items which the IoT connects to digital worlds include actuators, sensors, electronic toll devices in vehicles, washing machines, lighting systems, front door locks, thermometers, air conditioning units, and many more (Atzori et al., 2010; Kopetz, 2011; Xia et al., 2012; Greengard, 2016; Wortmann and Flüchter, 2015). A global survey showed that 43% of responding companies planned to implement IoT initiatives by the end of 2016 (Gartner, 2016). By evolving the IoT technology, testing and deploying products, we should be much close to achieving smart environments by 2021 (Misra et al., 2017).

Recent IoT data protocols are specifically designed for IoT devices such as NB-IoT, LoraWan, or Sigfox, all of which use low-power wide-area networks to connect at a low bit rate a large number of devices with low energy consumption and low cost (Postscapes, 2015). As presented by Lee and Lee (2015), IoT technologies that are essential in the deployment of successful IoT-based products and services are classified into five categories as radio-frequency identification (RFID), wireless sensor networks (WSN), middleware, cloud computing, and IoT applications. Researchers expect that the IoT must be available at a low cost in a large number of objects (Kamal et al., 2017). However, some find that the IoT faces several challenges such as scalability, self-organizing, data volumes, data interpretation, interoperability, automatic discovery, software complexity, security and privacy issues, fault tolerance, power supply, and wireless communications (Davies, 2015; Kamal et al., 2017).

Even though the future IoT could enable everyone access to and rich information about things and locations, several developments in the IoT have concentrated on the combination of Auto-ID and networked infrastructures in logistics and product life cycle applications (Uckelmann et al., 2011). Sun (2012) claims that enterprises with the IoT could monitor their every product in real time – without the need for the products to appear in the line of sight – and manage their logistics architecture. Since these companies can analyze the information generated from every procedure and forecast, their ability to respond to market needs can greatly improve (Sun, 2012). Wortmann and Fluchter (2015) discuss that existing business models might have to be adapted or redefined based on the new positioning of products in the IoT, and even entire industry boundaries may need to be reassessed in today's competitive marketplace. Furthermore, new marketing tools and modern design principles may be required to support the development of a connected product (Fleisch et al., 2014; Heppelmann and Porter, 2014). Moreover, IoT offers new technologies related to cloud and distributed computing, big data, and security issues to develop smarter applications as soon (Chong et al., 2013). Therefore, we should discover the security issues of IoT-based procurement, production, and distribution processes.

Smart Supply Chain Management Using the IoT

The application of IoT concepts in supply chains management processes is still a new issue. The uses of RFID in supply chain management between 2000–2015 are presented by Musa and Dabo (2016). They claim that despite technical and cost challenges, there is still enormous potential for the application of RFID in several areas of supply chain management. Liu et al. (2017) conducted a systematic review of the IoT literature regarding infrastructures, enabling technologies, potential technologies, and research challenges showing its multidimensional development and chances for revolutionizing the economy in the next years.

Generally, most agree that the IoT enabling technologies usually consist of four main layers: a data collection layer using mainly RFID objects and sensors; a transmission layer such as fixed and mobile networks; a service layer; and an interface layer (Ping et al., 2011; Gubbi et al., 2013; Borgia, 2014; Ben-Daya et al., 2019). The IoT can aid supply chain management in several areas such as cost-saving, inventory accuracy, and product tracking (Ben-Daya et al., 2019). Since the goods need to be monitored, they should be tracked indoors by developing the RFID positioning system, and outdoors by mainly using GPS (Yuvaraj and Sangeetha, 2016). Tao et al. (2014) design an IoT-based framework to achieve intelligent perception and access to various manufacturing resources. Gnimpieba et al. (2015) propose the architecture of a platform based on advanced technologies related to the IoT for better collaboration and interoperability enhancement in supply chains. According to this approach, instead of individually responding to orders, it would be better if suppliers could reorganize themselves by collaborating and sharing more data to better respond to all market demands (Ajay, 2012). Moreover, based on the IoT architecture, Shih and Wang (2016) present a time-temperature indicator to control the temperature of a cold supply chain.

Some authors identify relevant challenges to the IoT development such as the scalability of the Internet, the identification and addressing of billions of "things," and the heterogeneity of "things" and service paradigms (Antonowicz and Jarzębowski, 2018;

Haller et al., 2009). Furthermore, security and privacy issues are further elaborated by Bi et al. (2014) and Agrawal and Lal Das (2011). El Khodr et al. (2013) tend to various attack vectors for privacy attacks in the IoT and implications of these attacks on user privacy. Moreover, Bui (2011) discusses IoT-enabling technologies, including communication protocols, identification, object platforms, security, and privacy.

In light of the IoT's impact on supply chain functions, Yu et al. (2015) posit that the influence of both hard and soft infrastructure on customer satisfaction is fully mediated by flexibility. Decker et al. (2008) describe several benefits of the IoT connected to sourcing, and they develop a simple linear cost model to examine the impact of sensors and alerts on the unit purchase cost. Zawadzki and Żywicki (2016) declare that smart design and production control are necessary elements of a smart factory that is to be able to implement the mass customization strategy. Others find that smart manufacturing leads to smarter decisions and more efficient operations through factory and supply chain visibility based on real-time information (Ben-Daya et al., 2019). Dweekat et al. (2017) present a practical supply chain performance measurement approach and highlight the promising role of the IoT in performance measurement in general. Kumar et al. (2016) develop an integrative framework to understand the interplay between smart city technological initiatives – including big data analytics – and the industrial IoT and distributed manufacturing on supply chain design. Xu (2011) argues that successful supply chain quality management relies on increasingly sophisticated systems, highlighting key technologies that have the potential to significantly improve this area. Chen (2015) proposes the intelligent IoT-enabled system in the green supply chain to simulate a complex system through linked physical and digital objects with relationships. Yan et al. (2014) present an intelligent supply chain integration and management system to provide flexible and agile approaches for the facilitation of resource sharing and participant collaboration in the whole supply chain life cycle. Trab et al. (2015) represent an improvement key for decentralized management of warehouses in a dynamic and reactive environment. Moreover, they define IoT-based negotiations mechanisms and multi-agent systems to solve the security problem of product allocation operations. Zhiduan (2005) proposes using an information-sharing platform for the electronic waste recovery in supply chains through an electronic product code. Parry et al. (2016) demonstrate how the IoT might be operationalized in a domestic setting to capture data about consumers' use of products, which introduces implications for reverse supply chains. Liu et al. (2016) propose a project regarding the agricultural IoT, which is to integrate state-of-the-art technologies to provide a method for simple tracking supply processes of foods so as to counter the food safety problem. Wang and Yue (2017) propose a food safety pre-warning system by adopting association rule mining and the IoT in order to timely monitor all detection data of the whole supply chain and automatically issue warnings.

As the above section shows, the IoT's impact on supply chain management appears in various processes. However, there remain several gaps to be dealt with in IoT applications for supply chain management, specifically regarding security issues. Therefore, this study explored supply chain management's security criteria – including IoT technologies – by investigating supply chain systems of 10 selected companies from the FMCG industry.

Smart Supply Chain Security Criteria

Security and privacy are significant constraints to the popularity and acceptance of the IoT. The nature of IoT vulnerabilities illustrates the need for security and privacy in IoT design. Along with a technological model for security, a foolproof IoT ecosystem would also require a reconsideration of related governance, economics, and social ethics (Misra et al., 2017). One of the biggest challenges in protecting the IoT infrastructure is heterogeneity because the highly constrained devices that operate in low power and lossy network standards are required to open secure communication channels with more powerful devices on the Internet by using standard Internet protocols (Gutierrez et al., 2001; Roman et al., 2011). Thus, key management is an indispensable element of a secure network infrastructure. An efficient key management mechanism for the IoT should consider its heterogeneity and resource-constrained members. Such a key management mechanism should support a large device population and high dynamics of the IoT environment (Roman et al., 2011).

In order to check the security of IoT systems, important security indicators must be identified in the system. The ways that can be sources of data generation and transmission should be carefully considered. Given the importance of the subject under study, all processes in the supply chain that were associated with the production, reception, and transmission of data were first investigated (in the supply chain of food and pharmaceutical companies). Then, using the literature review and experts' opinions, we analyzed the security criteria for supply chains. The following will introduce the security measures of the smart supply chain.

The four supply chain security criteria have been developed from the literature review and experts' opinions, and then seventeen sub-criteria were identified.

Reliability. In the IoT context, there are several reliability threats that can affect those attributes. The IoT devices are deployed everywhere, and attackers can mount attacks remotely via network interfaces and physically, e.g. by performing dynamic fault induction or by collecting information through side-channels (Joye and Tunstall, 2012; Mangard et al., 2007). The IoT is a complex system in which many devices with continuously updated software and services cooperate using a dynamically changing communication network and in which the number of devices is not known in advance. These properties make IoT applications prone to design and implementation flaws, but also scaling bugs. Given the vast number of performed operations within the IoT platform in the supply chain, reliability is crucial from the security perspective. The most critical sub-criteria are trust, integrity, responsiveness, availability, and resistance to attack in reliability criterion.

Service. In the field of IoT, the produced data is extensive. This much data should be available concurrently and should not overlap. At the same time, the data must adequately authenticate the users who may be in other clusters. A security incident like damages to the integrity or availability can affect any IoT protocol or component, causing an impact that can be categorized as reputational, operative, or legal (López et al., 2018). The reputational impact refers to the damage of the image of the IoT service, and it will have consequences such as loss of IoT user trust or widespread lack of subscriptions. Due to momentary activities in the supply chain – especially in the FMCG industry – the availability, integration, and synchronization of services can be essential. In the service criterion, the most significant sub-criteria are service availability, service trust, authentication, reputation, and access control.

Network. Several IoT applications may cooperate with each other to accomplish specific tasks or services (Abdulghani et al., 2019). Anonymous services are operational, and they are not designed for user interaction (Ammar et al., 2018). The existence of robust networks capable of simultaneous processing is one of the most important parts of the IoT and must be kept anonymous while preserving utmost accuracy. Supply chain processes are widespread in different sectors and require strong networks. In the network criterion, the most critical sub-criteria are anonymization, network availability, and network integrity.

Privacy. Customers use their smartphones, tablets, or laptops to interact with other IoT devices indirectly either through a cloud backend or a gateway (Ammar et al., 2018). Moreover, IoT devices can provide information to manufacturers about the living environment and customer needs. On the other hand, suppliers can interact with companies and organizations through their information systems and their relationship with IoT (Abdel-Basset et al., 2018). Privacy in the infrastructure and all services offered in different sectors form further key measures in the security of supply chains that operate on IoT platforms (Calatayud et al., 2019). In the privacy criterion, the most critical sub-criteria are infrastructure confidentiality, service privacy, customer privacy, and supplier privacy. Figure 1 provides a hierarchical tree of criteria and sub-criteria.

Methodology

The research method used in this study was survey research. In terms of its purpose, this study was applied to introduce and apply fuzzy nonlinear mathematical modeling to rank the smart supply chain management (SSCM). Moreover, the study sought solutions for understanding the security criteria of an intelligent supply chain.

For this study, we selected companies from the FMCG industry in Iran due to the vastness and generality of the industry, but also the importance of supply chain and agile distribution in their delivery network structure. Among the studied companies, those affected by the IoT at the beginning of 2020 were primarily active in the food and pharmaceutical industries. Therefore, three pharmaceutical companies and seven food-producing companies were selected as the sample.

Much information was collected through interviews and questionnaires completed by experts in the fields under study – 35 experts, 25 supply chain specialists, and 10 IT specialists – with more than five years of experience in supply chain management or information technology. Next, data adequacy was confirmed using the Kaiser–Mayer–Olkin (KMO) test in SPSS. Then, questionnaires were sent to the experts. The questionnaires' rate of incompatibility was calculated using expert choice software. The results proved that the data was reliable.

The solution method was conceptual modeling with the group fuzzy preference programming method. Data collection was done through library studies, and field variables were measured. In order to converge the answers for the reliability of the questionnaires, we tried to visually monitor the dispersion of experts' answers. In summary, the evaluation framework of this research consisted of the four following stages.

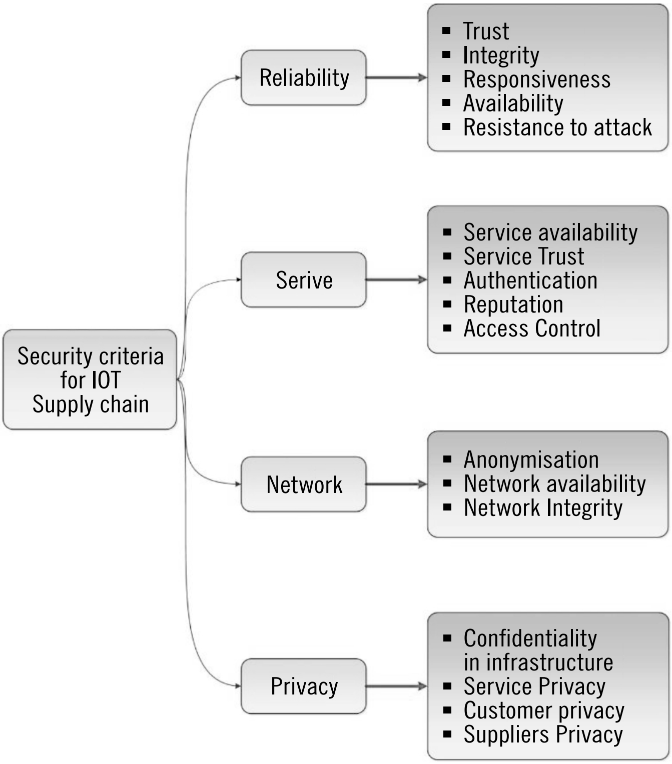
Step 1. Identifying and evaluating security criteria in the smart supply chain (IoT-based). In this study, we first attempted to examine the security criteria in the IoT supply chain thoroughly by using the literature review of the subject and related articles in the world's scientific databases. Then, by employing the views of supply chain experts

DOI: 10.7206/cemj.2658-0845.63

and IT professionals, four criteria (reliability, service, network, and privacy) were selected as potential key security criteria in the IoT supply chain and sub-criteria were also identified.

Step 2. Hierarchical tree drawing. At this stage, the hierarchical structure of the decision was plotted using objective, criteria, and options levels (Figure 1).

Figure 1. Security criteria in IoT supply chain



Source: own elaboration.

Step 3. Fuzzy judgment matrix formation. The consensus matrices of fuzzy judgments were based on decision-makers' views. Therefore, we had to use fuzzy numbers in explaining people's preferences and opinions.

Step 4. Mathematical modeling. In this study, the fuzzy nonlinear mathematical model was used to rank the criteria based on pairwise comparisons in the analytic hierarchy process (AHP) method. In this case, the model was solved using the upper and lower boundaries of the pairwise comparison matrix layers.

Below, we will briefly present the methods and concepts used in this study.

The new group fuzzy preference programming (GFPP) method was used to derive group priorities from crisp pairwise comparison judgments given by multiple decision-makers (Mikhailov and Singh, 1999). Consider a group of K decision-makers (DMs), comparing pairwisely *n* elements at the same level of the analytic hierarchy process (AHP) hierarchy. Each DM provided a set of crisp comparison judgments, $A_k = \{a_{ijk} \mid i = 1, 2,...; n - 1, j = 2, 3,..., n\}, k = 1, 2,..., K,$ in which a_{ijk} represented the relative e importance of the decision element E_i over E_j, concerning an upper-level element, as assessed by the *k* DM.

To apply these relationships, the fuzzy judgment agreement matrices had to be formed according to experts' opinions. Therefore, we had to use fuzzy numbers to identify people's preferences and surveys. Next, we could use the following nonlinear formulation of the group prioritization problem. To this end, we needed to formulate and solve this model using the upper and lower boundaries of the matrix layers:

$$\begin{aligned} &\max \lambda \\ &s.t: (m_{ij} - l_{ij})\lambda w_j - w_i + l_{ij} w_j \leq 0 \\ &\quad (u_{ij} - m_{ij})\lambda w_j + w_i - u_{ij} w_j \leq 0 \\ &\quad \sum_{k=1}^{n} w_k = 1 \\ &w_k > 0 \quad , k = 1,2,\ldots,n \;; \quad i = 1,2,\ldots,n-1 \;; \; j = 2,3,\ldots,n \quad , \; j > i \end{aligned} \tag{1}$$

The pairwise comparisons matrix was obtained by using the analytic hierarchy process method (Mikhailov, 2000) and by integrating expert opinions. Fuzzy linguistic scales were used to obtain expert opinions. These linguistic scales for the matrix of pairwise comparisons and their fuzzy equations are shown in Table 1.

Table 1. Linguistic criteria for pairwise comparisons and their fuzzy equivalents

Linguistic criterion	Triangular fuzzy scales
Very low	(1, 2, 3)
Low	(2, 3, 4)
Medium	(3, 4, 5)
High	(4, 5, 6)
Very high	(5, 6, 7)

Source: own elaboration.

The optimum positive value of the indicator in relation 1 revealed that all weight ratios were entirely true to the original judgment. However, if the indicator was negative, we could see that fuzzy judgments were strongly incompatible.

Results

Fuzzy mathematical modeling based on AHP was used to evaluate and rank the criteria obtained by employing field and study methods. For this purpose, 35 specialists in the FMCG industry (25 supply chain specialists and 10 IT specialists) were selected to fill the prepared questionnaires. Then, experts were asked to use paired comparisons using linguistic criteria (Table 1) to analyze the security criteria of the IoT-based supply chain. Thus, the evaluation and ranking of IoT supply chain security criteria in FMCG companies were divided into two parts:

(1) The fuzzy pairwise comparison matrix determination was based on the integration of expert opinions expressed according to linguistic criteria presented in Table 1.
(2) Solving the proposed nonlinear mathematical model (Relation 1) used pairwise comparison matrices, which provided the weight of security criteria.

The pairwise comparisons matrix for IoT-based supply chain security criteria and sub-criteria – based on the integration of experts' opinions – is shown in Tables 2 to 6. We used these paired comparisons for our calculations in the mathematical model.

Table 2. Paired comparison matrix of security criteria in the IoT supply chain, based on experts' opinions

	Reliability			Service			Network			Privacy		
	W1			W2			W3			W4		
W1	–	–	–	–	–	–	–	–	–	–	–	–
W2	6	5.1	5.1	–	–	–	–	–	–	–	–	–
W3	2.7	4.3	5.4	4.9	1.9	4.9	–	–	–	–	–	–
W4	4.1	4.23	5	2.4	5.8	3.4	2.08	1.8	3.1	–	–	–

Source: own elaboration.

Table 3. Paired comparison matrix of security sub-criteria of reliability, based on experts opinions

	Trust			Integrity			Responsiveness			Availability			Resistance to attack		
	W1			W2			W3			W4			W5		
W1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
W2	1.2	1.55	1.9	–	–	–	–	–	–	–	–	–	–	–	–
W3	2.25	2.75	3.9	2.25	2.75	7.25	–	–	–	–	–	–	–	–	–
W4	1.5	1.75	2.75	1.25	1.25	5.55	1	1.25	1.1	–	–	–	–	–	–
W5	1.11	2.1	3.15	1.25	1.20	3.9	0.85	1.25	1.25	1.25	1.25	2	–	–	–

Source: own elaboration.

Table 4. Paired comparison matrix of security sub-criteria of service, based on experts opinions

	Service availability			Service Trust			Authentication			Reputation			Access Control		
	W1			W2			W3			W4			W5		
W1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
W2	1.75	1.75	2	–	–	–	–	–	–	–	–	–	–	–	–
W3	1.25	2.75	4	1.64	2.69	6.55	–	–	–	–	–	–	–	–	–
W4	1.11	1.76	2.7	1.1	1.7	5.25	1	1.5	1.1	–	–	–	–	–	–
W5	2.15	1.29	2.51	1.21	1.25	4	1.25	1	1.24	1.24	2.4	1.5	–	–	–

Source: own elaboration.

DOI: 10.7206/cemj.2658-0845.63

Table 5. Paired comparison matrix of security sub-criteria of the network, based on experts opinions

	Anonymisation			Network availability			Network Integrity		
	W1			**W2**			**W3**		
W1	–	–	–	–	–	–	–	–	–
W2	2.8	3	5.5	–	–	–	–	–	–
W3	3.1	3.2	4.1	2.1	1.5	4	–	–	–

Source: own elaboration.

Table 6. Paired comparison matrix of security sub-criteria of privacy, based on experts opinions

	Confidentiality in infrastructure			Service Privacy			Customer privacy			Suppliers Privacy		
	W1			**W2**			**W3**			**W4**		
W1	–	–	–	–	–	–	–	–	–	–	–	–
W2	4.5	3	6	–	–	–	–	–	–	–	–	–
W3	4	4	7	3	2.5	6	–	–	–	–	–	–
W4	2.5	4	4.5	3	6.5	4.1	2	2	3.5	–	–	–

Source: own elaboration.

After performing pairwise comparisons of expert opinions on different sections, the data from these matrices were used in mathematical modeling to rank. Fuzzy values were put in the mathematical model. Since the model was nonlinear, we used the LINGO software to solve the model. Thus, the weight and rank of the criteria and sub-criteria were obtained, provided in Tables 7 to 11.

After calculating the weights of each metric and sub-criteria, we could normalize the weights using the information in Tables 7 to 11. The normalized weight for the IoT supply chain security sub-criteria is shown in Figure 2. The normalized weight represents the overall rank of the sub-criteria as a whole.

Table 7. Weight of security criteria of IoT supply chain (taken from the fuzzy nonlinear model)

Security Criteria	code	Weight	rank
Reliability	W1	0.3684722	1
Service	W2	0.1384005	4
Network	W3	0.1760491	3
Privacy	W4	0.3170783	2

Source: own elaboration.

Table 8. Weight of security sub-criteria in reliability (taken from the fuzzy nonlinear model)

Security sub-criteria	code	Weight	rank
Trust	W1	0.163246	3
Integrity	W2	0.113245	5
Responsiveness	W3	0.302313	1
Availability	W4	0.278875	2
Resistance to attack	W5	0.142321	4

Source: own elaboration.

Table 9. Weight of security sub-criteria in service (taken from the fuzzy nonlinear model)

Security sub-criteria	code	Weight	rank
Service availability	W1	0.254321	2
Service Trust	W2	0.163246	4
Authentication	W3	0.272132	1
Reputation	W4	0.204357	3
Access Control	W5	0.105944	5

Source: own elaboration.

DOI: 10.7206/cemj.2658-0845.63

Table 10. Weight of security sub-criteria in the network (taken from the fuzzy nonlinear model)

Security sub-criteria	code	Weight	rank
Anonymisation	W1	0.113246	3
Network availability	W2	0.414023	2
Network Integrity	W3	0.512135	1

Source: own elaboration.

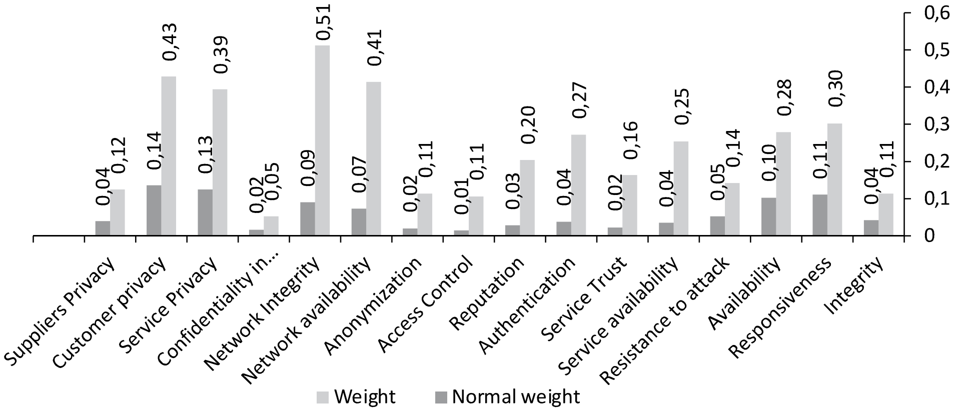
Table 11. Weight of security sub-criteria in privacy (taken from the fuzzy nonlinear model)

Security sub-criteria	code	Weight	rank
Confidentiality in infrastructure	W1	0.052801	4
Service Privacy	W2	0.394322	2
Customer privacy	W3	0.428342	1
Suppliers Privacy	W4	0.124536	3

Source: own elaboration.

Figure 2 shows that the reliability and privacy criteria emerged as more important than other criteria because the former have a higher weight than the latter.

Figure 2. Normalized weight and rating of IoT supply chain security criteria and sub-criteria



Source: own elaboration.

Discussion and Conclusion

The concept of “smart technologies” has expanded in recent years as a new form of sustainable development, and it represents models that incorporate all alternative approaches for improving the quality and performance of services to better engage all stakeholders in processes. Thus, new solutions that help smarten homes, organizations, and processes are fundamental today. Since the need for intelligence in the supply chain is one of the most vital parts of organizations, attention to this section and digitalization actions can be of great importance. Therefore, this article attempted to explore the IoT concept and its relation to the supply chain. The IoT integrates physical and digital structures while providing a whole new level of big data applications and services.

In this case, as a vast amount of data is moving in this platform, supply chain security can be crucial. To this end, we studied the security of the IoT-based supply chain by examining the factors affecting the supply chain to identify smart supply chain security. The study population consisted of companies from the FMCG industry due to the nature of production and the importance of supply chain processes in these industries. In order to check supply chain security criteria, questionnaires were sent to the specialists working in these companies. Then, to evaluate the importance of each security criterion and sub-criterion of the IoT supply chain (in FMCG industries) and based on the results of the pairwise comparisons matrix and the integration of expert opinions, we solved a nonlinear mathematical model and determined the weight and significance of each criterion.

Research results show that reliability and privacy are the most critical security criteria in the IoT supply chain. Therefore, professionals and experts in the IT and supply chain must pay more attention to these two criteria. From a security viewpoint, customer and service privacy is of paramount importance that requires much more attention. When analyzing the share of individual sub-criteria in the reliability criterion, responsiveness, availability, and trust appeared to have the greatest importance.

Like in any new technology, also in the IoT-based supply chain, there are no universal practices or best solutions for every sector. However, our study answers which security criteria are the most important for the experts of the surveyed companies. The chosen experts have significant experience to assess the importance of particular criteria since they know the processes of IoT-based supply chain management and the main obstacles appearing while carrying out particular tasks. Our study can help to create safe solutions in this area because the mentioned technologies are relatively new and still evolving, so the companies implementing them are constantly creating various new solutions to build secure supply chains using the IoT.

The results of this study can be used both in the practice of protecting devices in the IoT-based supply chain – but also in theoretical work. The IoT is a network of people, processes, data, things, and applications connected to the Internet. The interconnected elements – both physical and social – create a network, exchange data, collect data, and interact (Lee and Lee, 2015). Such a large and multidimensional accumulation of interactions is exceptional and unique. Hence, the importance of maintaining consumer privacy, service privacy, and supplier privacy is clear and confirmed by the study. This importance is even more understandable as the IoT operates in the "Unseen Internet," whose users are often unaware that data can be easily transferred and collected. In the Unseen Internet, decisions can be made even without user recognition, which is why maintaining privacy is so important. Thus, the use of the IoT in the supply chain – as a relatively new and undiscovered technology – must be conducted with the utmost care for safety.

One of the greatest advantages of the IoT-based supply chain is minimizing the number of supplies. On the other hand, this approach involves significant risk in the case of delayed deliveries, hence the significant role of the reliability of adopted solutions. Any interruption in the IoT-based supply chain will have greater consequences for consumers, producers, and suppliers, than in the traditional supply chain.

The IoT-based supply chain means not only the integration of vertical and horizontal value chains but also their digitalization. Integration processes in the horizontal dimension are processes in individual organizations: from design and purchasing through deliveries to after-sales services. In a vertical dimension, they include the interaction with suppliers, customers, and other co-operators in the value chain (Wang et al., 2016). This multidimensional integration within many co-operators causes the increasing importance of the reliability and safety of the system.

In the IoT-based supply chain, what is crucial is the immediate and undisturbed flow of a great amount of information on products and actors involved in the process. All actors want to cooperate closely by integrating their systems, which can enable them to optimize their supply chains. Nevertheless, each entity simultaneously wants to take care of its privacy and data security. Therefore, in the creation of an IoT-based supply chain, we should consider the expectations of people involved in implementing the (already functioning) smart supply chains. This article provides such recommendations at the beginning of this section.

Despite the scientific and managerial implications of the results, the study has some limitations, mainly regarding the sample size and the sampling process (purposive sampling). The group of surveyed companies from the FMCG industry was small, so the future studies should be more extensive so that one could extrapolate their results for the whole population of companies in the scrutinized industry. Moreover, this study provides only an insight into the limited scope of the FMCG industry, namely pharmaceuticals and food. Therefore, this is only an initial insight, not a whole new theory. However, our study could prove useful to decision-makers and researchers by bringing a new perspective on developing contemporary supply chains. Supply chains in the FMCG industry are very specific due to the speed of delivery and the characteristics of products. Nevertheless, more research is necessary to check the most critical security criteria in the IoT-based supply chains in other industries.

Therefore, we recommend widening the study scopes in the future. Responses can be collected from other industries as well as from lower-level managers. The latter's work is not so specialized but they have multiple practical skills regarding supply chain security in the operational dimension (not tactical or strategic). Moreover, the sample size is one of the limitations that could be increased by extending the coverage to more companies, also located in other countries. Our study was based on companies from one country (Iran), which does not present any differences in the legal, cultural, or business environment, which may have weighed on the study results.

Nevertheless, this study can be a strong reference point for other articles and a foundation for similar future studies. We hope that this article will encourage other researchers to develop the theory of the IoT-based supply chain, especially in the area of security criteria. The IoT in supply chains will develop dynamically in the coming years, and data security is of increasing importance in economic life, not only in supply chains.

References

Abdel-Basset, M., Manogaran, G., and Mohamed, M. (2018). Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. *Future Generation Computer Systems, 86*. https://doi.org/10.1016/j.future.2018.04.051.

Abdulghani, H.A., Nijdam, N.A., Collen, A., and Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective. *Symmetry, 11*(6). https://doi.org/10.3390/sym11060774.

Agrawal, S. and Das, M.L. (2011). *Internet of things – A paradigm shift of future internet applications. 2011 Nirma University International Conference on Engineering: Current Trends in Technology, NUiCONE 2011 – Conference Proceedings*. https://doi.org/10.1109/NUiConE.2011.6153246.

Ajay, S. (2012). Designing a Demand Driven Supply Network. *Research, LBS Journal of Management, 10*(2), 35–40.

Ammar, M., Russello, G. and Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*. https://doi.org/10.1016/j.jisa.2017.11.002.

Antonowicz, M. and Jarzębowski, S. (2018). Innovative models of supply chain management. *Journal of Management and Business Administration. Central Europe*, *26*(2), 2–15.

Ashton, K. (2009). That Internet of Things Thing. *RFID Journal*, *4986*.

Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15). https://doi.org/10.1016/j.comnet.2010.05.010.

Ben-Daya, M., Hassini, E. and Bahroun, Z. (2019). Internet of things and supply chain management: a literature review. *International Journal of Production Research*. https://doi.org/10.1080/00207543.2017.1402140.

Bi, Z., Xu, L. Da, and Wang, C. (2014). Internet of things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics*, *10*(2). https://doi.org/10.1109/TII.2014.2300338.

Bibri, S.E. (2018). The IoT for smart sustainable cities of the future : An analytical framework for sensor-based big data applications for environmental sustainability. *Sustainable Cities and Society*, *38*, 230–253.

Bibri, S.E. and Krogstie, J. (2017). On the social shaping dimensions of smart sustainable cities: A study in science, technology, and society. *Sustainable Cities and Society, 29*. https://doi.org/10.1016/j.scs.2016.11.004.

Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. *Computer Communications*. https://doi.org/10.1016/j.comcom.2014.09.008.

Bui, N. (2011). *Internet of Things Architecture (IoT-A). Project Deliverable D1.2 – Initial Architectura Reference Model for IoT L.*

Calatayud, A., Mangan, J. and Christopher, M. (2019). The self-thinking supply chain. *Supply Chain Management*, *24*(1). https://doi.org/10.1108/SCM-03-2018-0136.

Chen, R.Y. (2015). Intelligent IoT-Enabled System in Green Supply Chain using Integrated FCM Method. *International Journal of Business Analytics, 2*. https://doi.org/10.4018/IJBAN.2015070104.

Chong, Z.J., Qin, B., Bandyopadhyay, T., Wongpiromsarn, T., Rebsamen, B., Dai, P., Rankin, E.S., et al. (2013). Autonomy for mobility on demand. *Intelligent Autonomous Systems. Advances in Intelligent Systems and Computing*, Springer Verlag, Berlin Heidelberg, 671–682.

David, D.R., Nait-Sidi-moh, A., Durand, D. and Fortin, J. (2015). Using Internet of Things technologies for a collaborative supply chain: Application to tracking of pallets and containers. *Procedia Computer Science*, *56*. https://doi.org/10.1016/j.procs.2015.07.251.

Davies, R. (2015). The Internet of Things Opportunities and Challenges. *European Parliament Briefing*, May.

Decker, C., Berchtold, M., Chaves, L.W.F., Beigl, M., Roehr, D., Riedel, T., Beuster, M., et al. (2008). Cost-benefit model for smart items in the supply chain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4952 LNCS. https://doi.org/10.1007/978-3-540-78731-0_10.

Dobroszek, J. and Szychta, A. (2015). Indicators as an Instrument of Measurement in Management Accounting in Logistics Enterprises in Poland. *Management and Business Administration. Central Europe*, *23*(4), 11–33.

Dweekat, A.J., Hwang, G. and Park, J. (2017). A supply chain performance measurement approach using the internet of things: Toward more practical SCPMS. *Industrial Management and Data Systems*, *117*(2). https://doi.org/10.1108/IMDS-03-2016-0096.

Ellis, S., Morris, H.D. and Santagate, J. (2015). IoT-Enabled Analytic Applications Revolutionize Supply Chain Planning and Execution (White Paper). *International Data Corporation (IDC) White Paper*, November.

Fleisch, E., Weinberger, M. and Wortmann, F. (2014). Business Models and the Internet of Things. *Bosch IoT Lab White Paper*.

Gartner (2016). Survey Analysis: Early Adopters of Internet of Things Poised to Make 2016 the Year of the Customer. *Gartner*, No. G00298428.

Gnimpieba, Z.D.R., Nait-Sidi-Moh, A., Durand, D. et al. (2015). Using Internet of Things technologies for a collaborative supply chain: Application to tracking of pallets and containers. *Procedia Computer Science*, *56*(1), 550–557. http://dx.doi.org/10.1016/j.procs.2015.07.251.

Greengard, S. (2016). Internet of Things. *International Journal of Communication*, *10*.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7). https://doi.org/10.1016/j.future.2013.01.010.

Gutierrez, J.A., Naeve, M., Callaway, E., Bourgeois, M., Mitter, V. and Heile, B. (2001). IEEE 802.15.4: A developing standard for low-power low-cost wireless personal area networks. *IEEE Network*. https://doi.org/10.1109/65.953229.

Haller, S., Karnouskos, S. and Schroth, C. (2009). The Internet of things in an enterprise context. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5468*. https://doi.org/10.1007/978-3-642-00985-3_2.

Heppelmann, J.E. and Porter, M. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*, *11*(November).

Joye, M. and Tunstall, M. (2012). *Fault Analysis in Cryptography. Information Security and Cryptography*. Berlin Heidelberg: Springer Verlag.

Kamal, Z., Mohammed, A., Sayed, E. and Ahmed, A. (2017). Internet of Things Applications, Challenges and Related Future Technologies. *World Scientific News*, *67*(2).

El Khodr, M., Shahrestani, S., and Cheung, H. (2013). *The Internet of Things: Vision and Challenges*. IEEE TENCON Spring Conference, IEEE, Sydney, 1–8.

Kopetz, H. (2011). Internet of Things, Real-Time Systems. *International Journal of Innovations & Advancement in Computer Science*, *3*(8).

Kumar, M., Graham, G., Hennelly, P. and Srai, J. (2016). How will smart city production systems transform supply chain design: a product-level investigation. *International Journal of Production Research*, *54*(23). https://doi.org/10.1080/00207543.2016.1198057.

Lee, I. and Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4). https://doi.org/10.1016/j.bushor.2015.03.008.

Li, L. (2011). *Application of the internet of thing in green agricultural products supply chain management. Proceedings – 4th International Conference on Intelligent Computation Technology and Automation, ICICTA 2011*, *1*. https://doi.org/10.1109/ICICTA.2011.256.

Liu, F., Tan, C.W., Lim, E.T.K. and Choi, B. (2017). Traversing knowledge networks: an algorithmic historiography of extant literature on the Internet of Things (IoT). *Journal of Management Analytics*. https://doi.org/10.1080/23270012.2016.1214540.

Liu, Y., Han, W., Zhang, Y., Li, L., Wang, J. and Zheng, L. (2016). An Internet-of-Things solution for food safety and quality control: A pilot project in China. *Journal of Industrial Information Integration*, *3*. https://doi.org/10.1016/j.jii.2016.06.001.

López, D.D., Uribe, M.B., Cely, C.S., Murgueitio, D.T., Garcia, E.G., Nespoli, P. and Mármol, F.G. (2018). Developing secure IoT services: A security-oriented review of IoT platforms. *Symmetry*, *10*(12). https://doi.org/10.3390/sym10120669.

Mangard, S., Oswald, E. and Popp, T. (2007). *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. https://doi.org/10.1007/978-0-387-38162-6.

Mikhailov, L. (2000). A Fuzzy Programming Method for Deriving Priorities in the Analytic Hierarchy Process. *The Journal of the Operational Research Society*, *51*(3). https://doi.org/10.2307/254092.

Mikhailov, L. and Singh, M.G. (1999). Fuzzy assessment of priorities with application to competitive bidding. *Journal of Decision Systems*, *8*(1). https://doi.org/10.1080/12460125.1999.10511753.

Misra, S., Maheswaran, M. and Hashmi, S. (2017). *Security Challenges and Approaches in Internet of Things*, *Cutter IT Journal*, *29*.

Musa, A. and Dabo, A.A.A. (2016). A Review of RFID in Supply Chain Management: 2000–2015. *Global Journal of Flexible Systems Management*, *17*(2). https://doi.org/10.1007/s40171-016-0136-2.

Parry, G.C., Brax, S.A., Maull, R.S. and Ng, I.C.L. (2016). Operationalising IoT for reverse supply: the development of use-visibility measures. *Supply Chain Management*, *21*(2). https://doi.org/10.1108/SCM-10-2015-0386.

Ping, L., Liu, Q., Zhou, Z. and Wang, H. (2011). Agile supply chain management over the Internet of Things. *International Conference on Management and Service Science, MASS 2011*. https://doi.org/10.1109/ICMSS.2011.05998314.

Postscapes (2015). IoT Standards and Protocols. *Postscapes*.

Roman, R., Najera, P. and Lopez, J. (2011). Securing the Internet of things. *Computer*, *44*(9). https://doi.org/10.1109/MC.2011.291.

Sarma, S., Brock, D. and Ashton, K. (2000). *The networked physical world*. Cambridge: MIT.

Schliwa, G., Armitage, R., Aziz, S., Evans, J. and Rhoades, J. (2015). Sustainable city logistics – Making cargo cycles viable for urban freight transport. *Research in Transportation Business and Management*, *15*, 50–57.

Shih, C.W. and Wang, C.H. (2016). Integrating wireless sensor networks with statistical quality control to develop a cold chain system in food industries. *Computer Standards and Interfaces*, *45*. https://doi.org/10.1016/j.csi.2015.12.004.

Sun, C. (2012). Application of RFID Technology for Logistics on Internet of Things. *AASRI Procedia*, *1*. https://doi.org/10.1016/j.aasri.2012.06.019.

Tao, F., Zuo, Y., Xu, L. Da and Zhang, L. (2014). IoT-Based intelligent perception and access of manufacturing resource toward cloud manufacturing. *IEEE Transactions on Industrial Informatics*, *10*(2). https://doi.org/10.1109/TII.2014.2306397.

Trab, S., Bajic, E., Zouinkhi, A., Abdelkrim, M.N., Chekir, H. and Ltaief, R.H. (2015). Product Allocation Planning with Safety Compatibility Constraints in IoT-based Warehouse. *Procedia Computer Science*, *73*. https://doi.org/10.1016/j.procs.2015.12.033.

Uckelmann, D., Harrison, M. and Michahelles, F. (2011). An Architectural Approach Towards the Future Internet of Things. *Architecting the Internet of Things*. https://doi.org/10.1007/978-3-642-19157-2_1.

Vongsingthong, S. and Smanchat, S. (2014). Internet of Things: a Review of Applications. *Suranaree Journal of Science & Technology, 21*(4).

Wang, J. and Yue, H. (2017). Food safety pre-warning system based on data mining for a sustainable food supply chain. *Food Control, 73*. https://doi.org/10.1016/j.foodcont.2016.09.048.

Wang, S., Wan, J., Li, D., and Zhang, Ch. (2016). Implementing Smart Factory of Industrie 4.0: An outlook. *International Journal of Distributed Sensor Networks, 16*(7), 1–10.

Wortmann, F. and Flüchter, K. (2015). Internet of Things: Technology and Value Added. *Business and Information Systems Engineering*. https://doi.org/10.1007/s12599-015-0383-3.

Xia, F., Yang, L., Wang, L. and Vinel, A. (2012). Internet of Things. *International Journal Of Communication Systems, 25*(9), 1101–1102.

Xu, L. Da. (2011). Information architecture for supply chain quality management. *International Journal of Production Research, 49*(1). https://doi.org/10.1080/00207543.2010.508944.

Yan, J., Xin, S., Liu, Q., Xu, W., Yang, L., Fan, L., Chen, B., et al. (2014). Intelligent supply chain integration and management based on cloud of things. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1155/2014/624839.

Yu, J., Subramanian, N., Ning, K. and Edwards, D. (2015). Product delivery service provider selection and customer satisfaction in the era of internet of things: A Chinese e-retailers' perspective. *International Journal of Production Economics, 159*. https://doi.org/10.1016/j.ijpe.2014.09.031.

Yuvaraj, S. and Sangeetha, M. (2016). *Smart supply chain management using internet of things(IoT) and low power wireless communication systems*. Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016. https://doi.org/10.1109/WiSPNET.2016.7566196.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1). https://doi.org/10.1109/JIOT.2014.2306328.

Zawadzki, P. and Zywicki, K. (2016). Smart product design and production control for effective mass customization in the industry 4.0 concept. *Management and Production Engineering Review, 7*(3). https://doi.org/10.1515/mper-2016-0030.

Zhiduan, X. (2005). Research on the Flexibility in Logistic Systems. *Chinese Journal of Management, 4*, 441–445.