GESTÃO & PRODUÇÃO

ISSN 0104-530X (Print)
ISSN 1806-9649 (Online)

Thematic Section

Digital transformation, intelligent manufacturing and supply chain management 4.0

Supply Chain 4.0 challenges

Desafios da Supply Chain 4.0

Felipe de Campos Martins[1], Alexandre Tadeu Simon[1], Renan Stenico de Campos[1]

[1]Universidade Metodista de Piracicaba – UNIMEP, Faculdade de Engenharia, Arquitetura e Urbanismo, Programa de Pós-graduação em Engenharia de Produção, Santa Bárbara d'Oeste, SP, Brasil. E-mail: felipe_dcm@hotmail.com; alexandre.simon@unimep.br; renanstenico@hotmail.com

How to cite: Martins, F. C., Simon, A. T., & Campos, R. S. (2020). Supply Chain 4.0 challenges. *Gestão & Produção*, 27(3), e5427. https://doi.org/10.1590/0104-530X5427-20

Abstract: The Supply Chain has undergone major transformations due to the need to implement new Industry 4.0 technologies, such as Internet of Things, Big Data, Cyber-Physical Systems and Cloud Computing. Thanks to these technologies, as well as to their subsystems and components, full integration of the supply chain is becoming possible. However, it is observed that the real impacts of Industry 4.0 technologies, rather positive or negative, are not yet totally clear and identified. This paper aims to identify and present an analysis of the challenges and obstacles that Industry 4.0 technologies may cause in the Supply Chain. For this, the most relevant papers on the topic were selected and analyzed through a systematic literature review. Twenty challenges grouped into four macrogroups were identified: (1) technical challenges, (2) financial, environmental and legal challenges, (3) technological challenges, and (4) sociocultural challenges. It should be noted that these challenges require greater attention and more in-depth studies on the part of the academy to support industry in order to mitigate them and thus allow better use of the available technological resources and optimize the performance of Supply Chain operations.

Keywords: Supply chain; Supply chain 4.0; Industry 4.0; Challenges.

Resumo: A *Supply Chain* vem passando por grandes transformações em função da necessidade de implementação de novas tecnologias da Indústria 4.0, como a Internet das Coisas, Big Data, Sistemas Físico-Cibernéticos e a Computação em Nuvem. Graças a essas tecnologias, bem como a seus subsistemas e componentes, a integração total da *Supply Chain* está se tornando possível. No entanto, observa-se que ainda não estão totalmente claros e identificados os reais impactos, positivos ou negativos, que as tecnologias da Indústria 4.0 causam na *Supply Chain*. Este trabalho tem como objetivo identificar e apresentar uma análise dos desafios que as empresas deverão enfrentar ao implantar as tecnologias da Indústria 4.0 na *Supply Chain*. Para isso, foram selecionados e analisados, por meio de uma revisão sistemática da literatura, os trabalhos mais relevantes sobre o tema. A revisão identificou vinte desafios agrupados em quatro macrogrupos: (1) desafios técnicos, (2) desafios financeiros, ambientais e legais, (3) desafios tecnológicos e (4) desafios socioculturais. Observa-se que estes desafios requerem grande atenção e estudos mais aprofundados por parte da academia para apoiar a indústria no sentido de mitigá-los e, assim, permitir melhor aproveitamento dos recursos tecnológicos disponíveis e otimizar o desempenho das operações da *Supply Chain.*

Palavras-chave: *Supply chain*; *Supply chain* 4.0; Indústria 4.0; Desafios.

Received Apr. 2, 2019 – Accepted Mar. 10, 2020
Financial support: This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

1 Introduction

Supply Chain (SC) has been intensively studied, and great efforts have been made to integrate and strengthen companies' competitiveness. Nevertheless, the SC function, which is responsible for coordinating both the internal activities of companies and the relationship between their customers and suppliers (Schrauf & Berttram, 2016), is becoming increasingly complex, making it difficult to improve companies' activities' performance and cost reduction (Fore et al., 2016). In this respect, integrating processes among SC members is essential. One way to achieve such integration lies in the use of innovative technologies (Butner, 2010).

This need to integrate SC processes is not new, and studies have been carried out at the two levels of SC integration: (a) interorganizational, integrating customers and suppliers; and (b) intraorganizational, covering the company's internal activities (Flynn et al., 2010).

Today, through the emergence of the fourth industrial revolution—better known as Industry 4.0—as a result of the strong integration of information and communication technologies to connect the physical world to the virtual world (Kagermann et al., 2013; Davies, 2015), there are great opportunities to integrate and connect companies and their respective resources in order to increase performance in terms of time, money, and resource use (Büyüközkan & Göçer, 2017). Schrauf & Berttram (2016) noted that integrating SC processes and making information transparent among customers and suppliers enable companies to engage in collaborative actions. This leads to increased flexibility, productivity, and quality as well as the possibility of optimizing their business processes (Davies, 2015; Rüßmann et al., 2015).

The digitalization of processes and activities of the SC, as a result of the application of the technologies of Industry 4.0, has gained more and more attention from industry and academia (Büyüközkan & Göçer, 2017). However, the real impacts of such technologies on SC (Tjahjono et al., 2017), whether positive or negative, are not totally clear and identified. Under this focus, this paper aims to identify and analyze the challenges that companies must face when implementing the technologies of Industry 4.0 in SC.

This work intends to provide a better understanding of the obstacles of using Industry 4.0 technologies in the SC. Once the problems are identified, new studies may focus on the minimization and/or elimination of these problems, allowing better results in integrating the SC and using the potential offered by technological innovations.

This paper is structured in five sections, including this introductory one. Section 2 presents the bibliographic review, contemplating a brief understanding of Supply Chain 4.0 (SC4.0). Section 3 presents the methodological procedures. Section 4 describes the results obtained in the study. Finally, section 5 presents the conclusions and future research opportunities.

2 Literature review

SC4.0 is defined as "[…] a series of interconnected activities concerned with coordination, planning and controlling of products and services between suppliers and consumers" (Büyüközkan & Göçer, 2017, p. 01). Its objective is to generate new ways of adding value for customers and suppliers and generating more revenue through the integration and coordination of its processes (Büyüközkan & Göçer, 2017; Tjahjono et al., 2017): forecasting, acquisition, manufacturing, distribution, and sales and marketing (Chan, 2003):

Six characteristics of SC4.0 that should cover all customers and suppliers that make up the supply chain are presented by Wu et al. (2016) in their work (Table 1).

Table 1. Characteristics of SC4.0.

CHARACTERISTICS	DESCRIPTION
Instrumented	Systems with sensors, RFID tags, meters and other integrated components capable of generating data for decision making.
Interconnected	Supply chain's members fully connected, including their assets, IT systems, products, and other smart objects.
Intelligent	Intelligent systems capable of making decisions in order to optimize their global performance by collecting and analyzing large volumes of data.
Automated	Numerous automated activities which aim to replace less efficient resources (including labor).
Integrated	Integrated supply chain activities, involving collaboration among members, making decisions together, making use of common systems and sharing information.
Inovative	Ability to develop and aggregate new values through more efficient solutions.

Source: Adapted by Wu et al. (2016).

These characteristics are due to technologies enabled by Industry 4.0. Four of these technologies are considered the technology basis of Industry 4.0: (Teimoury et al., 2013; Macaulay et al., 2015; Reddy et al., 2016).

The Internet of Things (IoT) aims to extend and connect physical objects to the Internet (Uckelmann et al., 2011) by integrating sensors, actuators, and other devices that collect, transmit, and process data (Khanna, 2016). In the SC, this technology brings business and Web applications (such as social media) together with machines, devices, products, materials, and people, making it possible to create an intelligent network that extends across all factory processes and customers and suppliers (Szozda, 2017).

Cyber-Physical systems comprise machines, storage systems, and production facilities that have been digitally developed and present end-to-end integration based on information and communication technologies (Kagermann et al., 2013). They are characterized by decentralization, adaptation, and autonomous behavior (Ivanov & Sokolov, 2012), and they offer SC opportunities to monitor conditions of manufacturing and logistics activities in real time, enabling prognosis and remote diagnosis and control (Lee et al., 2013).

Cloud computing aims to integrate technologies or architectures to provide a platform or solution through the Internet, allowing them to be accessed anytime and anywhere (Raza et al., 2015), generating unprecedented visibility, insights, and flexibility (Büyüközkan & Göçer, 2018).

Big data make up a large set of data from diverse sources, both traditional and digital, where analyses and continuous discoveries can be made (Arthur, 2013). Big data are distinguished in five dimensions—volume, variety, speed, veracity, and value (Yin & Kaynak, 2015)—and can be used for descriptive, predictive, and prescriptive analyses (Wang et al., 2016). In the SC, it presents applications that include material flows (such as production status, process and quality monitoring, inventory handling, logistics, research and development, and collective solutions in procurement and distribution functions), information flows (such as demand management, supply chain event management, vendor negotiation, risk management, problem identification, automated-decision support and customer management) and financial flows (such as customer segmentation, demand modeling, new business model design, pricing and assortment, and financial aspects of human resources).

Other technologies that impact the SC within Context 4.0 are also presented by Ghobakhloo (2018) and provide a source of competitive advantage for the SC: additive manufacturing, automation and industrial robots, augmented reality, cybernetic security, blockchain, Internet of data, people and services, semantic technologies, and simulation and modeling.

Thanks to these technologies and their subsystems and devices, it is possible to integrate the entire SC (not only customers and suppliers but also their assets, products, and operating environment) and generate a larger volume of data with more quality and speed (Wu et al., 2016). In addition, the technologies enable companies to increase flexibility, productivity, reliability, and responsiveness in their operations. Moreover, by enabling the reorganization of the entire operation in real time, companies have the possibility of reducing the bullwhip effect and costs associated with SC operations (Dweekat & Park, 2016).

3 Method

The systematic literature review method developed by Levy & Ellis (2006) was used to achieve the objective proposed in this work. The method consists of three steps as shown in Figure 1.

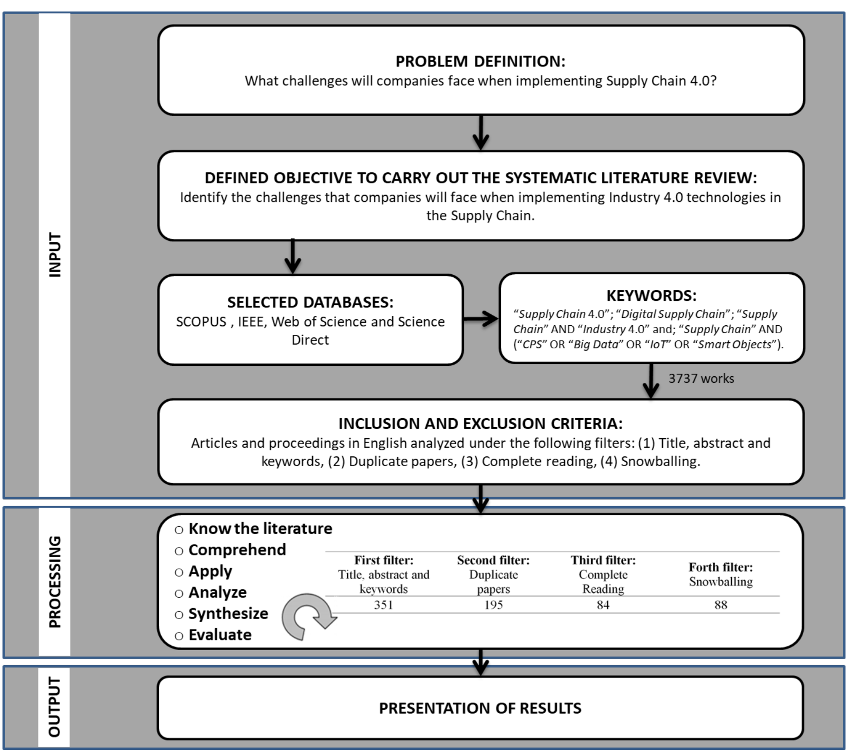

Figure 1. Systematic literature review process. Source: Adapted from Levy & Ellis (2006).

The first step, named *Input*, deals with search definitions, such as database choices, search strings, and inclusion and exclusion criteria. Four databases—SCOPUS, Web of Science, Science Direct, and IEEE—were used to search relevant papers about SC4.0 concepts. These databases were selected because they are considered the most important databases within the scope and area of the research. In each of the databases, four keyword groups were used to cover all relevant literature:

"Supply Chain 4.0";

"Supply Chain" AND "Industry 4.0";

"Digital Supply Chain" and;

"Supply Chain" AND ("CPS" OR "big data" OR "IoT" OR "smart objects").

Then the work was analyzed using three steps, as presented in Figure 2: (a) title, abstract and keywords; (b) duplicate papers; and (c) complete reading. In addition, it was considered a snowballing process to identify new papers which were not within the databases analyzed.

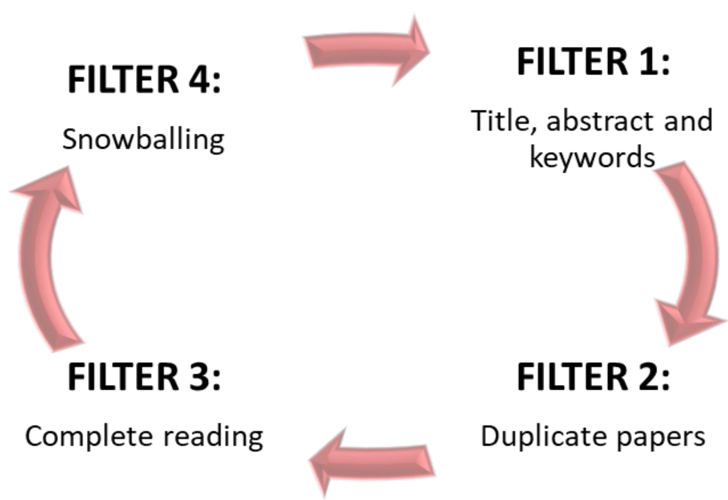

Figure 2. Steps of paper's analysis. Search: Authors.

Moreover, five criteria were considered for the inclusion or exclusion analysis of papers: (a) complete papers in the English language; (b) works that provide access to the full text; (c) academic, professional, or formal work (disregarding, for example, prefaces, personal views, and informal content based on the Internet, among others); (d) papers that focus on the theme SC4.0 or technologies related to its context, concentrating on the review, research, discussion, or solution of SC problems within the digital context; and (e) works where keywords used for document searches are the focus of the work, not just expressions quoted in them.

The second step, named *Processing*, is composed of six substeps, namely (a) knowing: identify the publications and extract their essential information; (b) understanding: understand the importance of the study performed and the result presented; (c) applying: identify the important concepts and categorize them accordingly; (d) analyzing: identify the relevance of the presented information; (e) synthesizing: integrate results to understand the concept in its entirety; and (f) evaluating: distinguish between opinions, theories, and instituted facts in an empirical way.

Finally, in the third step, *Outputs*, the results obtained through the method are presented.

4 Results and discussion

Through the use of the keywords presented in the previous section, 3,737 articles were identified in the databases, as presented in Table 2. The articles were analyzed according to the inclusion and exclusion criteria, resulting in a total of 88 selected papers. The quantities of articles filtered in each criterion are shown in Table 3.

Table 2. Number of articles identified in each search.

	"*Supply Chain 4.0*"	**"*Digital Supply Chain*"**	**"*Supply Chain*" AND "*Industry 4.0*"**	**"*Supply Chain*" AND ("*CPS*" OR "*Big Data*" OR "*IoT*" OR "*Smart objects*")**
SCOPUS	5	51	175	1046
Web of Science	1	18	110	705
Science Direct	2	9	44	145
IEEE	46	796	45	539

Source: Authors.

Table 3. Results of the systematic literature review process' steps.

First filter: Title, abstract and keywords	**Second filter: Duplicate papers**	**Third filter: Complete Reading**	**Forth filter: Snowballing**
351	195	84	88

Source: Authors.

When analyzing the 88 papers identified, it is observed that studies related to the challenges within the SC4.0's context have been growing and gaining more and more attention over the years. Moreover, studies done between 2016 and 2018 have concentrated the largest quantity of publications, as presented in Table 4. These numbers demonstrate the growing concern and search for solutions to minimize these challenges and maximize the benefits of this concept.

Table 4. Number of papers published per year.

Publication's year	**Number of papers**
2010	1
2011	2
2012	1
2013	5
2014	2
2015	12
2016	18
2017	25
2018	22

Source: Authors.

A preliminary analysis of the challenges makes it possible to classify them into four distinct macrogroups based on the similarities that they imply on their occurrence. Figure 3 shows the macrogroups and their respective challenges: (a) technological challenges; (b) financial, environmental, and legal challenges; (c) sociocultural challenges; and (d) technical challenges. Table 5 shows the percentage of articles and proceedings published that discuss the challenges of each macrogroup. Table 6 summarizes the challenges that companies face and/or will face when implementing the technologies of Industry 4.0 in the SC.

Table 5. Percentage of articles addressing the challenges according to classification.

Macrogroups	Amount of articles
Technological Challenges	12.50%
Financial, environmental and legal challenges	20.45%
Sociocultural Challenges	22.73%
Technical Challenges	86.36%

Source: Authors.

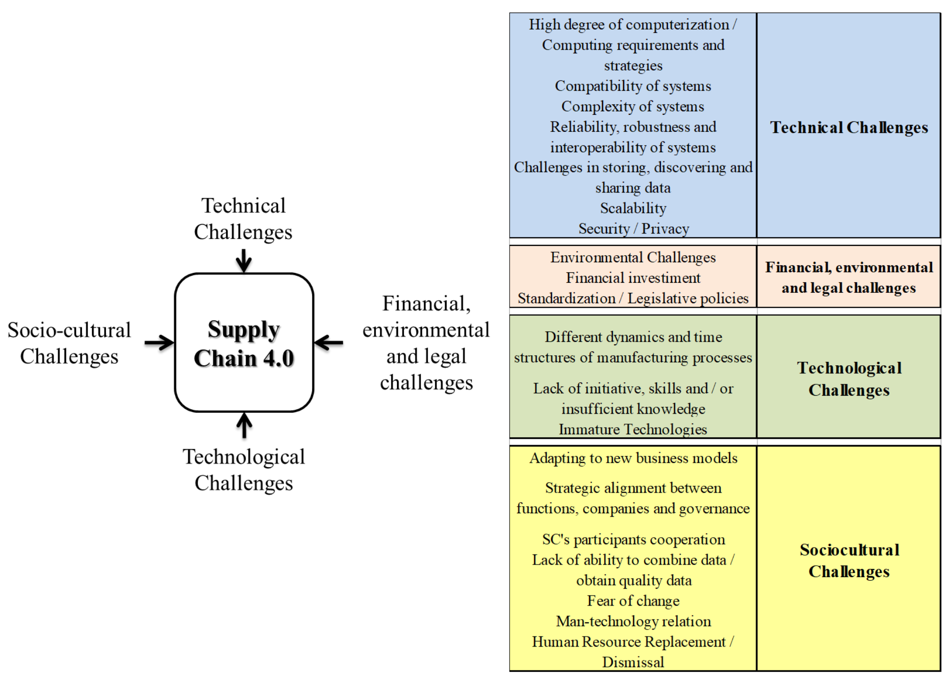

Figure 3. Supply Chain 4.0 challenges classification. Source: Authors.

Table 6. Challenges of Industry 4.0 Technologies in Supply Chain.

Challenges / Authors	High degree of computerization / Computing requirements and strategies	Compatibility	Complexity	Reliability, robustness and interoperability of systems	Challenges in storing, discovering and sharing data	Scalability	Security / privacy	Environmental Challenges	Financial investment	Standardization / Legislative policies	Different dynamics and time structures of manufacturing processes	Lack of initiative, skills and / or insufficient knowledge	Immature Technologies	Adapting to new business models	Strategic alignment between functions, companies and governance	SC's participants cooperation	Lack of ability to combine data / obtain quality data	Fear of change	Man-technology relation	Human Resource Replacement / Dismissal
Agrawal & Das (2011)							x													
Ahram et al. (2017)							x													
Alotaibi & Mehmood (2017)					x					x		x								
Amudhavel et al. (2015)					x		x													
Arya et al. (2017)			x			x						x					x			
Bailey et al. (2016)							x													
Barreto et al. (2017)							x													
Bhargava et al. (2013)							x													
Bienhaus & Haddud (2018)												x		x	x					
Burmester et al. (2017)							x													
Büyüközkan & Göçer (2018)				x			x		x	x						x	x		x	x
Casey & Wong (2017)										x										
National Cyber Security Centre (2015)							x													
Kumar Ch & Kameswara Rao (2018)							x													
Chang et al. (2017)							x													
Chamekh et al. (2017)							x													
Chen (2018)				x																
Chen et al. (2017)				x																

Table 6. Continued…

Challenges / **Authors**	**High degree of computerization / Computing requirements and strategies**	**Compatibility**	**Complexity**	**Reliability, robustness and interoperability of systems**	**Challenges in storing, discovering and sharing data**	**Scalability**	**Security / privacy**	**Environmental Challenges**	**Financial investment**	**Standardization / Legislative policies**	**Different dynamics and time structures of manufacturing processes**	**Lack of initiative, skills and / or insufficient knowledge**	**Immature Technologies**	**Adapting to new business models**	**Strategic alignment between functions, companies and governance**	**SC's participants cooperation**	**Lack of ability to combine data / obtain quality data**	**Fear of change**	**Man-technology relation**	**Human Resource Replacement / Dismissal**
Choi et al. (2018)	x																			
Chugh et al. (2016)							x													
Clancy (2017)																x				
Corici et al. (2016)							x													
Das (2015)							x													
Fraj et al. (2017)				x			x													
Gu (2018)				x	x															
Haddud et al. (2017)		x	x		x	x	x		x		x			x	x		x		x	x
Hallman et al. (2014)							x					x								
Harrison et al. (2016)		x							x											
He et al. (2016)							x													
Hiromoto et al. (2017)							x													
Isasi et al. (2015)					x					x						x				
Ivanov et al. (2016)											x									
Ivanov et al. (2016)											x									
Jeske et al. (2013)							x						x				x			
Kache & Seuring (2017)		x	x				x		x						x	x	x			
Kapoor et al. (2011)							x													
Khanna & Sharma (2017)			x				x			x					x					x
Kshetri (2017a)							x													
Kshetri (2017b)							x													
Kshetri (2018)	x																			
Kenny (2017)							x													

Table 6. Continued…

Challenges / Authors	High degree of computerization / Computing requirements and strategies	Compatibility	Complexity	Reliability, robustness and interoperability of systems	Challenges in storing, discovering and sharing data	Scalability	Security / privacy	Environmental Challenges	Financial investment	Standardization / Legislative policies	Different dynamics and time structures of manufacturing processes	Lack of initiative, skills and / or insufficient knowledge	Immature Technologies	Adapting to new business models	Strategic alignment between functions, companies and governance	SC's participants cooperation	Lack of ability to combine data / obtain quality data	Fear of change	Man-technology relation	Human Resource Replacement / Dismissal
Kumar et al. (2017)							x													
Kumar et al. (2013)			x														x			
Kynast & Marjanovic (2016)			x						x			x	x		x					
Lee & Kwon (2016)							x													
Lee & Lee (2015)			x		x		x										x			
Sánchez López et al. (2012)						x	x		x											
Lu et al. (2013)							x													
Luszcz (2017)							x													
Makhdoom et al. (2019)							x													
Mamun et al. (2018)							x													
McDonald et al. (2016)							x													
Miao & Zhang (2014)							x	x												
Mikavicaa et al. (2015)					x		x													
Mohr & Khan (2015)							x			x										
Moniem et al. (2017)							x													
Moyne et al. (2018)							x													
Mylrea & Gourisetti (2018)				x			x													
Omitola & Wills (2018)							x													
Ong et al. (2016)																	x			
Pearsall (2016)												x								
Pirpilidis et al. (2016)							x													
Pishdar et al. (2018)				x	x	x	x	x	x	x				x	x	x	x			

Table 6. Continued…

Challenges / Authors	High degree of computerization / Computing requirements and strategies	Compatibility	Complexity	Reliability, robustness and interoperability of systems	Challenges in storing, discovering and sharing data	Scalability	Security / privacy	Environmental Challenges	Financial investment	Standardization / Legislative policies	Different dynamics and time structures of manufacturing processes	Lack of initiative, skills and / or insufficient knowledge	Immature Technologies	Adapting to new business models	Strategic alignment between functions, companies and governance	SC's participants cooperation	Lack of ability to combine data / obtain quality data	Fear of change	Man-technology relation	Human Resource Replacement / Dismissal
Queiroz & Telles (2018)									x			x								
Qian et al. (2018)	x						x													
Ray & Bhadra (2016)							x													
Ray et al. (2018b)							x													
Ray et al. (2018a)							x													
Ray et al. (2015)							x													
Richey et al. (2016)							x													
Schneider et al. (2018)				x																
Song et al. (2018)																	x			
Spanaki et al. (2018)							x										x			
Szozda (2017)					x		x													
Tjahjono et al. (2017)										x									x	
Tu (2018)									x											
Tuptuk & Hailes (2018)							x													
Urquhart & McAuley (2018)							x			x										
Xu et al. (2013)		x	x		x															
Wang et al. (2016)																	x			
Wazid et al. (2018)							x													
Weber (2010)							x			x										
Wilding & Wheatley (2015)							x													
Wolfert et al. (2017)					x		x										x			
Wu et al. (2016)												x	x					x		

Table 6. Continued…

Challenges / Authors	High degree of computerization / Computing requirements and strategies	Compatibility	Complexity	Reliability, robustness and interoperability of systems	Challenges in storing, discovering and sharing data	Scalability	Security / privacy	Environmental Challenges	Financial investment	Standardization / Legislative policies	Different dynamics and time structures of manufacturing processes	Lack of initiative, skills and / or insufficient knowledge	Immature Technologies	Adapting to new business models	Strategic alignment between functions, companies and governance	SC's participants cooperation	Lack of ability to combine data / obtain quality data	Fear of change	Man-technology relation	Human Resource Replacement / Dismissal
Yang et al. (2015)							x													
Yang et al. (2017)				x			x													
Yang et al. (2018)							x													
Zhong et al. (2016)				x	x	x	x													

Source: Authors.

Regarding the technological challenges, a first barrier is the need to develop technologies leveraged by Industry 4.0, which are still at an early stage and require great strides to create solidity and generate greater benefits (Kynast & Marjanovic, 2016; Wu et al., 2016). Haddud et al. (2017) identified the different operations models between members of the SC, and Ivanov et al. (2016) recognized the different dynamics and temporal structures of manufacturing processes and equipment that can compromise the data's collection, analysis, and sharing as well as the programming of the entire production structure.

The various formats and structures of the data add problems to the analysis and use of the data. Nevertheless, questions related to the data and their sharing are still reasons for further studies and inquiries. As noted in Pearsall (2016), the kind of data needed to share and the real purpose of doing this along the entire SC are not clear.

In addition, the technical feasibility for implementing technologies such as big data the knowledge to use these data well were pointed out by Jeske et al. (2013), Kynast & Marjanovic (2016), and Hallman et al. (2014). Arya et al. (2017) emphasized the lack of data specialists for the development of potential technology. Moreover, Queiroz & Telles (2018) also identified the lack of knowledge of the potential of this technology within Brazilian territory.

Among those covering the studies that present other technologies, Bienhaus & Haddud (2018) highlighted the lack of specialists to leverage the digitization in companies. Already, Wu et al. (2016) pointed out that among barriers to developing intelligent applications in SC are the lack of initiative, skills, and knowledge in technologies as well as the immaturity of the SC4.0 concept and its initial stage of development.

In the macrogroup for financial, environmental, and legal challenges, several authors emphasized the high investment needed to implement such solutions (Büyüközkan & Göçer, 2018; Haddud et al., 2017; Harrison et al., 2016; Kache & Seuring, 2017; Kynast & Marjanovic, 2016; Sánchez López et al., 2012; Queiroz & Telles, 2018; Tu, 2018). Pishdar et al. (2018) emphasized that such investments to obtain data and services derived from these technologies will not always present financial returns.

Regarding the legislative policies, laws are needed to ensure the safety and integrity of people within this new environment in which humans and robots share spaces and work collaboratively both inside (Tjahjono et al., 2017) and outside the corporate environment (Büyüközkan & Göçer, 2018; Casey & Wong, 2017). In addition to that, international legislation is required to ensure security and privacy (Weber, 2010), to solve problems related to personal injury and product liability in case of failure (Mohr & Khan, 2015), and to share responsibility for the information (Alotaibi & Mehmood, 2017). The balance of legal obligations between infrastructure's providers and customers (Urquhart & McAuley, 2018) within the digital universe is also important to consider. Authors discussing big data and RFID technologies (Isasi et al., 2015) and IoT (Khanna & Sharma, 2017) addressed the problems of global standards aiming the compatibility between systems, where the lack of these standards can lead to difficulties in data's collection and use. Pishdar et al. (2018) highlighted the importance of the laws as a way to form the basis for the technologies' development: As noted in their study, the lack of legislation is a challenge that can bring on many others.

Miao & Zhang (2014) raised the environmental challenges' issue of Industry 4.0 technologies, such as greater energy consumption due to the increased use of electronic equipment and integrated systems in SC. Pishdar et al. (2018) also added their concern about the number of electronic components that will become obsolete and require replacement over time.

The lack of capacity to combine data and obtain quality data is one of the challenges in the macrogroup sociocultural challenges and should be taken into account by companies due to (Jeske et al., 2013; Pishdar et al., 2018):

The various existing communication patterns and formats (Kumar et al., 2013; Lee & Lee, 2015; Wang et al., 2016);

The different ways of collecting, storing, and combining the data (Ong et al., 2016);

The lack of IT professionals with knowledge of matching and using data appropriately (Kache & Seuring, 2017); and

The problems of synchronizing data and systems (Haddud et al., 2017) as well as their quality (Song et al., 2018; Spanaki et al., 2018).

Arya et al. (2017) and Büyüközkan & Göçer (2018) explained that these factors hinder the use of the data in its totality, which brings about a low return from the use of technologies.

Cooperating with the SC's participants implies difficulties that start from mutual adoption and investments in the technologies of Industry 4.0 (Büyüközkan & Göçer, 2018; Clancy, 2017; Kache & Seuring, 2017) and extend to the difficulty in sharing responsibilities for errors within the digital context (Pishdar et al., 2018). Additionally, authors cited the diversity of operational models and the lack of integration between functions (Haddud et al., 2017), the lack of SC's governance structure (Kache & Seuring, 2017), the lack of a strategy for the use of the technologies (Bienhaus & Haddud, 2018; Kynast & Marjanovic, 2016; Pishdar et al., 2018), and the lack of ability to adapt and integrate firms to this new digital business model (Haddud et al., 2017; Pishdar et al., 2018).

Khanna & Sharma (2017) discussed the difficulties faced by companies in finding technology solutions that meet their specific needs. Isasi et al. (2015) emphasized that the nonimplementation of technologies at all stages of the supply chain implies a loss of integration and visibility.

Finally, the resistance to accepting and learning to use new technologies, the ethics and safety issues of dividing the workspace with machines, the replacement of the workforce by technologies, and the fear of making use of intelligent applications in SC were also considered (Büyüközkan & Göçer, 2018; Haddud et al., 2017; Khanna & Sharma, 2017; Tjahjono et al., 2017; Wu et al., 2016).

Regarding the technical challenges, studies that highlighted the big data technology discussed in greater amount the challenges related to the data generation. These challenges begin with the search, fragmentation, and visualization of data (Mikavicaa et al., 2015) and extend to the need to interpret and obtain information with quality and to access and make this data visible to other members in the SC (Kynast & Marjanovic, 2016).

Authors such as Alotaibi & Mehmood (2017), Amudhavel et al. (2015), Isasi et al. (2015), and Wolfert et al. (2017) explained that challenges like storing, analyzing, and processing data using traditional methods are due to the volume, variety, and heterogeneity of the data.

In addition, the creation of a system capable of interpreting and presenting value information from the data is complex (Arya et al., 2017; Kumar et al., 2013) and requires strategy (Choi et al., 2018), a trained team (Kumar et al., 2013; Kache & Seuring, 2017), and infrastructure capable of supporting all computing needs (Kache & Seuring, 2017). Furthermore, Kache & Seuring (2017) elucidated that IT systems with different levels of maturity can bring efficiency and visibility challenges to the global network.

System scalability and robustness challenges related to the collection, analysis, and simultaneous transmission of data were cited by Arya et al. (2017) and Zhong et al. (2016). These authors also highlighted the stability and vulnerability in transmitting data to systems, especially when done via wireless network.

As addressed with big data technology, IoT and other digital applications present challenges in storing, discovering, and sharing data (Szozda, 2017; Xu et al., 2013) and problems with scalability and interoperability (Büyüközkan & Göçer, 2017; Pishdar et al., 2018). Lee & Lee (2015) and Xu et al. (2013) addressed compatibility challenges when connecting all systems in SC. Khanna & Sharma (2017) reinforced this idea, noting the difficulty of predicting failures and exemplifying a simple electrical failure as a cause of chain reactions to all interconnected firms.

Challenges related to the vulnerability, reliability, robustness, complexity, and compatibility of IoT and RFID systems were addressed in the work of Chen et al. (2017), Gu (2018), Haddud et al. (2017), and Yang et al. (2017).

Finally, CPS and other automation systems studied imply challenges such as integration, efficient information exchange (Chen et al., 2017), and validation of solutions within the SC—a theme that still needs to be explored (Harrison et al., 2016).

Within this macrogroup, a concern arises with the challenge of security and privacy, addressed in approximately 72% of papers. Security and privacy in the use of technologies (big data, RFID, Internet of Things, cyber-physical systems, among others) are challenges mentioned in a great number of publications and show the extent of this challenge that SC members will face when implementing technologies driven by Industry 4.0. National Cyber Security Centre (2015) supported this idea by explaining that different companies have different levels of security in their systems, and the lower level of security allows the exposure of all other companies connected through attacks and intrusions.

5 Conclusion

Industry 4.0 introduces a range of innovations that allow companies to increase the performance of their internal and external activities and thus gain competitive advantage. In the SC, a sector that presents difficulties in obtaining efficiency due to the complexity in managing its internal and external operations, technologies from this context allow greater integration between systems and company resources to generate global value—that means for the whole chain.

However, there are numerous challenges when analyzing the concept of SC4.0. Although coordinating internal activities, systems, and other resources of a company with its customers and suppliers allows obtaining benefits in performance, quality, and costs, it can also bring to the companies great challenges, especially with regard to security and privacy. For example, there are several studies that presented models, tools, and systems that seek to minimize the risks of improper data acquisition, leakage and unauthorized disclosure of information, and insertion of malicious software, among other challenges. However, none of these studies eliminated the risks altogether. In addition, while different systems and equipment are integrated within the SC, greater potential for failures and risks is observed.

Moreover, the full integration of the internal activities in SC functions and the activities of customers and suppliers requires greater synergy among companies and researchers regarding investments, studies, and further technology development. At present, studies report partial integrations of functions and activities. While the theme is still at an early stage of development, obtaining practical data for analysis and comparison with the theory is difficult.

Investments and efforts by the government are also needed to overcome challenges regarding legislation. Some challenges exist due to other causes. In this sense, the lack of regulations creates security problems and harms users, as well as leading to the development of other challenges.

This study contributed to identifying the challenges related to SC4.0. In all, 20 technical, sociocultural, technological and financial, environmental, and legal challenges require further studies to minimize them and even eliminate them when aiming to achieve full SC efficiency through the use of available technologies. For future work, companies should be consulted on how these challenges are perceived by them as a concern and decision factor in relation to the implementation process.

Acknowledgements

The authors would like to thank CAPES for the support provided during this research.

References

Agrawal, S., & Das, M. L. (2011). Internet of Things: a paradigm shift of future Internet applications. In *Proceedings of the Nirma University International Conference on Engineering* (pp. 1-7). Piscataway: IEEE. http://dx.doi.org/10.1109/NUiConE.2011.6153246.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. In *Proceedings of the IEEE Technology & Engineering Management Conference (TEMSCON)* (pp. 137-141). Piscataway: IEEE. http://dx.doi.org/10.1109/TEMSCON.2017.7998367.

Alotaibi, S., & Mehmood, R. (2017). Big data enabled healthcare supply chain management: opportunities and challenges. In *Proceedings of the International Conference on Smart Cities, Infrastructure, Technologies and Applications* (pp. 207-215). Cham: Springer.

Amudhavel, J., Padmapriya, V., Gowri, V., Lakshmipriya, K., Kumar, K. P., & Thiyagarajan, B. (2015). Perspectives, motivations and implications of big data analytics. In *Proceedings of the International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015)* (p. 34). New York: ACM. http://dx.doi.org/10.1145/2743065.2743099.

Arthur, L. (2013). *What is big data?* Forbes Magazine. Retrieved in 2018, July 08, from https://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data/#189fcc6d5c85.

Arya, V., Sharma, P., Singh, A., & Silva, P. T. M. (2017). An exploratory study on supply chain analytics applied to spare parts supply chain. *Benchmarking*, 24(6), 1571-1580. http://dx.doi.org/10.1108/BIJ-04-2016-0053.

Bailey, G., Moss, C., Whittaker, J. F., & Millette, A. L. (2016). *Digital supply chains: a frontside flip*. New York: Digital Supply Chain Institute. Retrieved in 2018, July 21, from https://www.thecge.net/dsci/</bok>

Barreto, L., Amaral, A., & Pereira, T. (2017). Industry 4.0 implications in logistics: an overview. *Procedia Manufacturing*, 13, 1245-1252. http://dx.doi.org/10.1016/j.promfg.2017.09.045.

Bhargava, B., Ranchal, R., & Othmane, L. B. (2013). Secure information sharing in digital supply chains. In *Proceedings of the 3rd IEEE International Advance Computing Conference (IACC)* (pp. 1636-1640). Piscataway: IEEE.

Bienhaus, F., & Haddud, A. (2018). Procurement 4.0: factors influencing the digitisation of procurement and supply chains. *Business Process Management Journal*, 24(4), 965-984. http://dx.doi.org/10.1108/BPMJ-06-2017-0139.

Burmester, M., Munilla, J., Ortiz, A., & Caballero-Gil, P. (2017). An RFID-based smart structure for the supply chain: resilient scanning proofs and ownership transfer with positive secrecy capacity channels. *Sensors*, 17(7), 1562. http://dx.doi.org/10.3390/s17071562. PMid:28677637.

Butner, K. (2010). The smarter supply chain of the future. *Strategy and Leadership*, 38(1), 22-31. http://dx.doi.org/10.1108/10878571011009859.

Büyüközkan, G., & Göçer, F. (2017). An extension of MOORA approach for group decision making based on interval valued intuitionistic fuzzy numbers in digital supply chain. In *Proceedings of the Joint 17th World Congress of International Fuzzy Systems Association and 9th International Conference on Soft Computing and Intelligent Systems (IFSA-SCIS)* (pp. 1-6). Piscataway: IEEE.

Büyüközkan, G., & Göçer, F. (2018). Digital supply chain: literature review and a proposed framework for future research. *Computers in Industry*, 97, 157-177. http://dx.doi.org/10.1016/j.compind.2018.02.010.

Casey, M., & Wong, P. (2017, 13 march). *Global supply chains are about to get better, thanks to blockchain*. Harvard Business Review.

Chamekh, M., Hamdi, M., & El Asmi, S. (2017). A new architecture for supply-chain management. In *Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 77-82). Piscataway: IEEE. http://dx.doi.org/10.1109/CCNC.2017.7983085.

Chan, F. T. S. (2003). Performance measurement in a supply chain. *International Journal of Advanced Manufacturing Technology*, 21(7), 534-548.

Chang, P. Y., Hwang, M. S., & Yang, C. C. (2017). A blockchain-based traceable certification system. In *Proceedings of the International Conference on Security with Intelligent Computing and Big-data Services* (pp. 363-369). Cham: Springer.

Chen, H., Xue, G., & Wang, Z. (2017). Efficient and reliable missing tag identification for large-scale RFID systems with unknown tags. *IEEE Internet of Things Journal*, 4(3), 736-748. http://dx.doi.org/10.1109/JIOT.2017.2664810.

Chen, R. Y. (2018). Intelligent predictive food traceability cyber physical system in agriculture food supply chain. *Journal of Physics: Conference Series*, 1026(1), 012017. http://dx.doi.org/10.1088/1742-6596/1026/1/012017.

Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. *Production and Operations Management*, 27(10), 1868-1883. http://dx.doi.org/10.1111/poms.12838.

Chugh, N., Kumar, A., & Aggarwal, A. (2016). Security aspects of a RFID-sensor integrated low-powered devices for internet-of-things. In *Proceedings of the Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 759-763). Piscataway: IEEE. http://dx.doi.org/10.1109/PDGC.2016.7913223.

Clancy, H. (2017, 6 february). *The blockchain's emerging role in sustainability*. GreenBiz.

Corici, A. A., Emmelmann, M., Luo, J., Shrestha, R., Corici, M., & Magedanz, T. (2016). IoT inter-security domain trust transfer and service dispatch solution. In *Proceedings of the IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 694-699). Piscataway: IEEE.

Das, M. L. (2015). Privacy and security challenges in internet of things (pp. 33-48). In *Proceedings of the International Conference on Distributed Computing and Internet Technology*. Cham: Springer.

Davies, R. (2015). *Industry 4.0: digitalisation for productivity and growth* (10 p.). Brussels: European Parliamentary Research Service.

Dweekat, A. J., & Park, J. (2016). Internet of Things-enabled supply chain performance measurement model. In *Proceedings of the 2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA)* (pp. 1-3). Piscataway: IEEE. http://dx.doi.org/10.1109/ICIMSA.2016.7504014.

Flynn, B. B., Huo, B., & Zhao, X. (2010). The impact of supply chain integration on performance: a contingency and configuration approach. *Journal of Operations Management*, 28(1), 58-71. http://dx.doi.org/10.1016/j.jom.2009.06.001.

Fore, V., Khanna, A., Tomar, R., & Mishra, A. (2016). Intelligent supply chain management system. In *Proceedings of the International Conference on Advances in Computing and Communication Engineering (ICACCE)* (pp. 296-302). Piscataway: IEEE. http://dx.doi.org/10.1109/ICACCE.2016.8073764.

Fraj, R. B., Beroulle, V., Fourty, N., & Meddeb, A. (2017). A global approach for the improvement of UHF RFID safety and security. In *Proceedings of the 12th International Conference on*

Design & Technology of Integrated Systems in Nanoscale Era (DTIS) (pp. 1-2). Piscataway: IEEE.

Ghobakhloo, M. (2018). The future of manufacturing industry: a strategic roadmap toward Industry 4.0. *Journal of Manufacturing Technology Management*

Gu, C. (2018). Fast discrepancy identification for RFID-enabled IoT networks. *IEEE Access: Practical Innovations, Open Solutions*, 6, 6194-6204. http://dx.doi.org/10.1109/ACCESS.2017.2785810.

Haddud, A., DeSouza, A., Khare, A., & Lee, H. (2017). Examining potential benefits and challenges associated with the Internet of Things integration in supply chains. *Journal of Manufacturing Technology Management*, 28(8), 1055-1085. http://dx.doi.org/10.1108/JMTM-05-2017-0094.

Hallman, S., Rakhimov, J., Plaisent, M., & Bernard, P. (2014) Big data: preconditions to productivity. In *Proceedings of the IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 727-731). Piscataway: IEEE.

Harrison, R., Vera, D., & Ahmad, B. (2016). Engineering methods and tools for cyber-physical automation systems. *Proceedings of the IEEE*, 104(5), 973-985. http://dx.doi.org/10.1109/JPROC.2015.2510665.

He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., & Gabrys, B. (2016). The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In *Proceedings of the IEEE Congress on Evolutionary Computation (CEC)* (pp. 1015-1021). Piscataway: IEEE. http://dx.doi.org/10.1109/CEC.2016.7743900.

Hiromoto, R. E., Haney, M., & Vakanski, A. (2017). A secure architecture for IoT with supply chain risk management. In *Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (pp. 431-435). Piscataway: IEEE.

Isasi, N. K. G., Frazzon, E. M., & Uriona, M. (2015). Big data and business analytics in the supply chain: a review of the literature. *IEEE Latin America Transactions*, 13(10), 3382-3391. http://dx.doi.org/10.1109/TLA.2015.7387245.

Ivanov, D., & Sokolov, B. (2012). The inter-disciplinary modelling of supply chains in the context of collaborative multi-structural cyber-physical networks. *Journal of Manufacturing Technology Management*, 23(8), 976-997.

Ivanov, D., Dolgui, A., Sokolov, B., Werner, F., & Ivanova, M. (2016). A dynamic model and an algorithm for short-term supply chain scheduling in the smart factory industry 4.0. *International Journal of Production Research*, 54(2), 386-402. http://dx.doi.org/10.1080/00207543.2014.999958.

Jeske, M., Grüner, M., & Weiß, F. (2013). *Big data in logistics: a DHL perspective on how to move beyond the hype*. Troisdorf: DHL Customer Solutions & Innovation.

Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management. *International Journal of Operations & Production Management*, 37(1), 10-36. http://dx.doi.org/10.1108/IJOPM-02-2015-0078.

Kagermann, H., Wajlster, W., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative INDUSTRY 4.0*. Alemanha: National Academy of Science and Engineering.

Kapoor, G., Zhou, W., & Piramuthu, S. (2011). Multi-tag and multi-owner RFID ownership transfer in supply chains. *Decision Support Systems*, 52(1), 258-270. http://dx.doi.org/10.1016/j.dss.2011.08.002.

Kenny, S. (2017). Strengthening the network security supply chain. *Computer Fraud & Security*, 2017(12), 11-14. http://dx.doi.org/10.1016/S1361-3723(17)30108-2.

Khanna, A. (2016). An architectural design for cloud of things. Facta universitatis-series. *Electronics and Energetics*, 29(3), 357-365.

Khanna, P., & Sharma, A. (2017, march). Integrating SCM with internet of things: implication on HR management. In *Proceedings of the 2nd International Conference on Internet of things and Cloud Computing* (p. 170). New York: ACM. http://dx.doi.org/10.1145/3018896.3056787.

Kshetri, N. (2017a). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027-1038. http://dx.doi.org/10.1016/j.telpol.2017.09.003.

Kshetri, N. (2017b). Can blockchain strengthen the internet of things? *IT Professional*, 19(4), 68-72. http://dx.doi.org/10.1109/MITP.2017.3051335.

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80-89. http://dx.doi.org/10.1016/j.ijinfomgt.2017.12.005.

Kumar Ch, M., & Kameswara Rao, M. (2018). Critical review attacks and countermeasures in internet of things enabled environments. *IACSIT International Journal of Engineering and Technology*, 7(2.7), 163-167. http://dx.doi.org/10.14419/ijet.v7i2.7.10284.

Kumar, A., Niu, F., & Ré, C. (2013). Hazy: making it easier to build and maintain big-data analytics. *Communications of the ACM*, 56(3), 40-49. http://dx.doi.org/10.1145/2428556.2428570.

Kumar, K. S., Rao, G. H., Sahoo, S., & Mahapatra, K. K. (2017). Secure split test techniques to prevent IC piracy for IoT devices. *Integration*, 58, 390-400. http://dx.doi.org/10.1016/j.vlsi.2016.09.004.

Kynast, M., & Marjanovic, O. (2016). Big data in supply chain management-applications, challenges and benefits. In *Proceedings of the 22nd Americas Conference on Information Systems*. San Diego: AMCIS.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431-440. http://dx.doi.org/10.1016/j.bushor.2015.03.008.

Lee, J., & Kwon, T. (2016). Secure dissemination of software updates for intelligent mobility in future wireless networks. *EURASIP Journal on Wireless Communications and Networking*, 2016(1), 250. http://dx.doi.org/10.1186/s13638-016-0746-6.

Lee, J., Lapira, E., Bagheri, B., & Kao, H. (2013). Recent advances and trends in predictive manufacturing systems in big data environment. *Manufacturing Letters*, 1(1), 38-41.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline*, 9, 181-213. http://dx.doi.org/10.28945/479.

Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y., & Yang, H. (2013, september). Next big thing in big data: the security of the ICT supply chain. In *Proceedings of the International Conference on Social Computing* (pp. 1066-1073). Piscataway: IEEE. http://dx.doi.org/10.1109/SocialCom.2013.172.

Luszcz, J. (2017). How maverick developers can create risk in the software and IoT supply chain. *Network Security*, 2017(8), 5-7. http://dx.doi.org/10.1016/S1353-4858(17)30080-6.

Macaulay, J., Buckalew, L., & Chung, G. (2015). Internet of things in logistics. *DHL Trend Res.*, 1(1), 1-27.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of threats to the internet of things. *IEEE Communications Surveys and Tutorials*, 21(2), 1636-1675. http://dx.doi.org/10.1109/COMST.2018.2874978.

Mamun, M. S. I., Ghorbani, A. A., Miyaji, A., & Nguyen, U. T. (2018). SupAUTH: a new approach to supply chain authentication for the IoT. *Computational Intelligence*, 34(2), 582-602. http://dx.doi.org/10.1111/coin.12164.

McDonald, J. T., Kim, Y. C., Andel, T. R., Forbes, M. A., & McVicar, J. (2016). Functional polymorphism for intellectual property protection. In *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 61-66). Piscataway: IEEE. http://dx.doi.org/10.1109/HST.2016.7495557.

Miao, X., & Zhang, D. (2014). The opportunity and challenge of Big Data's application in distribution grids. In *Proceedings of the China International Conference on Electricity Distribution (CICED)* (pp. 962-964). Piscataway: IEEE. http://dx.doi.org/10.1109/CICED.2014.6991847.

Mikavicaa, B., Kostić-Ljubisavljevića, A., & Radonjić, V. (2015). Big data: challenges and opportunities in logistics systems. In *Proceedings of the 2nd Logistics International Conference* (pp. 185-90). Belgrade: LOGIC.

Mohr, S., & Khan, O. (2015). 3D printing and its disruptive impacts on supply chains of the future. *Technology Innovation Management Review*, 5(11), 20-25. http://dx.doi.org/10.22215/timreview/942.

Moniem, S. A., Taha, S., & Hamza, H. S. (2017). An anonymous mutual authentication scheme for healthcare RFID systems. In *Proceedings of the IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (pp. 1-6). Piscataway: IEEE.

Moyne, J., Mashiro, S., & Gross, D. (2018). Determining a security roadmap for the microelectronics industry. In *Proceedings of the 29th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC)* (pp. 291-294). Piscataway: IEEE.

Mylrea, M., & Gourisetti, S. N. G. (2018). Blockchain for supply chain cybersecurity, optimization and compliance. In *Proceedings of the 2018 Resilience Week (RWS)* (pp. 70-76). Piscataway: IEEE.

National Cyber Security Centre – NCSC. (2015) *Cert-UK: cyber-security risks in the supply chain*. London. Retrieved in 2018, May 7, from https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-security-risks-in-the-supply-chain.pdf

Omitola, T., & Wills, G. (2018). Towards mapping the security challenges of the Internet of Things (IoT) supply chain. *Procedia Computer Science*, 126, 441-450. http://dx.doi.org/10.1016/j.procs.2018.07.278.

Ong, B. Y., Wen, R., & Zhang, A. N. (2016, december). Data blending in manufacturing and supply chains. In *Proceedings of the IEEE International Conference on Big Data (Big Data)* (pp. 3773-3778). Piscataway: IEEE.

Pearsall, K. (2016). Manufacturing supply chain challenges-globalization and IOT. In *Proceedings of the 6th Electronic System-Integration Technology Conference (ESTC)* (pp. 1-5). Piscataway: IEEE.

Pirpilidis, F., Voyiatzis, A. G., Pyrgas, L., & Kitsos, P. (2016). An efficient reconfigurable ring oscillator for hardware Trojan detection. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics* (p. 66). New York: ACM. http://dx.doi.org/10.1145/3003733.3003808.

Pishdar, M., Ghasemzadeh, F., Antucheviciene, J., & Saparauskas, J. (2018). Internet of things and its challenges in supply chain management: a rough strength-relation analysis method. *Economics and Management*, 21(2), 208-222. http://dx.doi.org/10.15240/tul/001/2018-2-014.

Qian, Y., Zeng, P., Shen, Z., & Choo, K. K. R. (2018). A lightweight path authentication protocol for RFID-based supply chains. In *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications; 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)* (pp. 1297-1302). Piscataway: IEEE.

Queiroz, M. M., & Telles, R. (2018). Big data analytics in supply chain and logistics: an empirical approach. *International Journal of Logistics Management*, 29(2), 767-783. http://dx.doi.org/10.1108/IJLM-05-2017-0116.

Ray, B., Abawajy, J., Chowdhury, M., & Alelaiwi, A. (2018a). Universal and secure object ownership transfer protocol for the Internet of Things. *Future Generation Computer Systems*, 78, 838-849. http://dx.doi.org/10.1016/j.future.2017.02.020.

Ray, B., Howdhury, M., Abawajy, J., & Jesmin, M. (2015). Secure object tracking protocol for Networked RFID Systems. In *Proceedings of the IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 1-7). Piscataway: IEEE.

Ray, S., & Bhadra, J. (2016). Security challenges in mobile and IoT systems. In *Proceedings of the 29th IEEE International System-on-Chip Conference (SOCC)* (pp. 356-361). Piscataway: IEEE.

Ray, S., Chen, W., & Cammarota, R. (2018b). Protecting the supply chain for automotives and IoTs. In *Proceedings of the 55th ACM/ESDA/IEEE Design Automation Conference (DAC)* (pp. 1-4). Piscataway: IEEE.

Raza, M. H., Adenola, A. F., Nafarieh, A., & Robertson, W. (2015). The slow adoption of cloud computing and IT workforce. *Procedia Computer Science*, 52, 1114-1119.

Reddy, G. R. K., Singh, H., & Hariharan, S. (2016). Supply chain wide transformation of traditional industry to industry 4.0. *Journal of Engineering and Applied Sciences*, 11(18), 11089-11097.

Richey, R. G., Jr., Morgan, T. R., Lindsey-Hall, K., & Adams, F. G. (2016). A global exploration of big data in the supply chain. *International Journal of Physical Distribution & Logistics Management*, 46(8), 710-739. http://dx.doi.org/10.1108/IJPDLM-05-2016-0134.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). *Industry 4.0: the future of productivity and growth in manufacturing industries*. Boston: Boston Consulting Group.

Sánchez López, T., Ranasinghe, D. C., Harrison, M., & McFarlane, D. (2012). Adding sense to the internet of things: an architecture framework for smart object systems. *Personal and Ubiquitous Computing*, 16(3), 291-308. http://dx.doi.org/10.1007/s00779-011-0399-8.

Schneider, G., Keil, S., & Luhn, G. (2018). Opportunities, challenges and use cases of digitization within the semiconductor industry. In *Proceedings of the 29th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC)* (pp. 307-312). Piscataway: IEEE.

Schrauf, S., & Berttram, P. (2016, 7 september). *Industry 4.0: how digitization makes the supply chain more efficient, agile, and customer-focused*. Strategy&.

Song, M. L., Fisher, R., Wang, J. L., & Cui, L. B. (2018). Environmental performance evaluation with big data: theories and methods. *Annals of Operations Research*, 270(1-2), 459-472. http://dx.doi.org/10.1007/s10479-016-2158-8.

Spanaki, K., Gürgüç, Z., Adams, R., & Mulligan, C. (2018). Data supply chain (DSC): research synthesis and future directions. *International Journal of Production Research*, 56(13), 4447-4466. http://dx.doi.org/10.1080/00207543.2017.1399222.

Szozda, N. (2017). Industry 4.0 and its impact on the functioning of supply chains. *Logforum*, 13(4), 401-414.

Teimoury, E., Fathian, M., & Chambar, I. (2013). Automation of the supply chain performance measurement based on multi-agent system. *International Journal of Agile Systems and Management*, 6(1), 25-42. http://dx.doi.org/10.1504/IJASM.2013.052225.

Tjahjono, B., Esplugues, C., Ares, E., & Pelaez, G. (2017). What does industry 4.0 mean to supply chain? *Procedia Manufacturing*, 13, 1175-1182. http://dx.doi.org/10.1016/j.promfg.2017.09.191.

Tu, M. (2018). An exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management: a mixed research approach. *International Journal of Logistics Management*, 29(1), 131-151. http://dx.doi.org/10.1108/IJLM-11-2016-0274.

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, 47, 93-106. http://dx.doi.org/10.1016/j.jmsy.2018.04.007.

Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards the future internet of things. In: D. Uckelmann, M. Harrison & F. Michahelles (Eds.), *Architecting the internet of things* (p. 1-24). Springer, Berlin, Heidelberg.

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law & Security Review*, 34(3), 450-466. http://dx.doi.org/10.1016/j.clsr.2017.12.004.

Wang, Y., Hulstijn, J., & Tan, Y. H. (2016). Data quality assurance in international supply chains: an application of the value cycle approach to customs reporting. *International Journal of Advanced Logistics*, 5(2), 76-85. http://dx.doi.org/10.1080/2287108X.2016.1178501.

Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2018). Design of secure user authenticated key management protocol for generic iot networks. *IEEE Internet of Things Journal*, 5(1), 269-282. http://dx.doi.org/10.1109/JIOT.2017.2780232.

Weber, R. H. (2010). Internet of Things-New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30. http://dx.doi.org/10.1016/j.clsr.2009.11.008.

Wilding, R., & Wheatley, M. (2015). Q&A: how can i secure my digital supply chain? *Technology Innovation Management Review*, 5(4), 40-43. http://dx.doi.org/10.22215/timreview/890.

Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M. J. (2017). Big data in smart farming: a review. *Agricultural Systems*, 153, 69-80. http://dx.doi.org/10.1016/j.agsy.2017.01.023.

Wu, L., Yue, X., Jin, A., & Yen, D. C. (2016). Smart supply chain management: a review and implications for future research. *International Journal of Logistics Management*, 27(2), 395-417. http://dx.doi.org/10.1108/IJLM-02-2014-0035.

Xu, R., Yang, L., & Yang, S. H. (2013). Architecture design of internet of things in logistics management for emergency response. In *Proceedings of the IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing* (pp. 395-402). Piscataway: IEEE. http://dx.doi.org/10.1109/GreenCom-iThings-CPSCom.2013.85.

Yang, K., Forte, D., & Tehranipoor, M. (2018). ReSC: an RFID-enabled solution for defending ioT supply chain. *ACM Transactions on Design Automation of Electronic Systems*, 23(3), 29. http://dx.doi.org/10.1145/3174850.

Yang, K., Forte, D., & Tehranipoor, M. M. (2015). Protecting endpoint devices in IoT supply chain. In *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design* (pp. 351-356). Piscataway: IEEE. http://dx.doi.org/10.1109/ICCAD.2015.7372591.

Yang, K., Forte, D., & Tehranipoor, M. M. (2017). Cdta: a comprehensive solution for counterfeit detection, traceability, and authentication in the iot supply chain. *ACM Transactions on Design Automation of Electronic Systems*, 22(3), 42. http://dx.doi.org/10.1145/3005346.

Yin, S., & Kaynak, O. (2015). Big data for modern industry: challenges and trends [point of view]. *Proceedings of the IEEE*, 103(2), 143-146.

Zhong, R. Y., Newman, S. T., Huang, G. Q., & Lan, S. (2016). Big Data for supply chain management in the service and manufacturing sectors: challenges, opportunities, and future perspectives. *Computers & Industrial Engineering*, 101, 572-591. http://dx.doi.org/10.1016/j.cie.2016.07.013.