ISSN: 2783-2678

International journal of Innovation in Management Economics and Social Sciences

Journal homepage: www.ijimes.ir

Int. J. Inn. Man. Eco. Soc. Sci. Vol. 2, No 1, 52-64. (2022)

Assessment of Cyber Risks in an IoT-based Supply Chain using a Fuzzy Decision-Making Method

Hamed Nozari[1], Javid Ghahremani-Nahr[2‡], Mohammad Fallah[1], Agnieszka Szmelter-jarosz[3]

[1] Department of Industrial Engineering, Islamic Azad University, Central Tehran Branch,Tehran, Iran
[2] Faculty Member of Academic Center for Education, Culture and Research (ACECR), Tabriz, Iran
[3]Department of Logistics, Faculty of Economics, University of Gdańsk, Poland

ARTICLE INFO

Received: 10 December 2021

Reviewed: 20 December 2021

Revised:20 January 2022

Accept: 25 January 2022

Keywords: Cyber Risks, IoT based Supply Chain, Smart Supply Chain, Fuzzy Decision-Making Method.

ABSTRACT

Purpose: The Internet of Things (IoT) is a relatively new paradigm that is growing rapidly in modern wireless communication scenarios. The main idea of this concept is the pervasive presence of all kinds of objects around us. This technology is the basis of today's intelligent life and is known as one of the most important sources of big data. Meanwhile, businesses are no exception to this rule and try to use the Internet of Things to make their business smarter. Supply chain management is a goal-based goal of linking business operations to provide a common view of market opportunity.
Methodology: Using IoT technology, all major parts of the supply chain, including supply, production, distribution and sales, can be affected. Because this evolutionary technology is intertwined with Internet technology, the use of network-based tools can always create risks for business owners who use these technologies. Therefore, understanding and investigating a variety of cyber risks in this area can It is very important and by understanding their hands, we can prevent many future risks. Linear analysis based on hierarchical analysis is used.
Findings: The results show that privacy is very important in interaction with suppliers as well as customers, and therefore those effective measures to deal with these risks can reduce many of the problems caused by this technology.
Originality/Value: This paper attend to assessment of cyber risks in an IoT-based supply chain using a fuzzy decision-making method.

‡ Corresponding Author: javidgahremani1369@gmail.com
https://doi.org/10.52547/ijimes.2.1.52

1. Introduction

Today, with the increasing growth of technology, the form of business and business interactions with customers has changed completely. The technology and prosperity of the Internet has led to the emergence of new businesses and businesses, transforming many traditional businesses into the use of the Internet. Analysis and presentation of business data are used. Facilitating and optimizing the decision-making process, identifying business opportunities, increasing information sharing, communicating more effectively with customers, increasing the ability to prepare diverse and dynamic reports, and predicting the future of the organization are some of the benefits of smart business. [1]. The smart business environment is always dealing with a huge amount of data and this has created many challenges and opportunities. New information sources provide opportunities for new programs to improve the quality of activities. Investigating data from activities in different sectors of business has attracted interest from research communities in a variety of fields including data mining, energy and environmental sciences, social sciences, optimization, planning and transportation.

Internet-of-thing (IoT) technology, as one of the largest sources of massive data generation, plays a very important role in business intelligence. However, producing, storing, maintenance and processing of this data will always have many challenges. Data privacy and security is a major concern for them. Social networking and data sharing, the uses of smartphones that dominate the most private sectors of today's life and many other challenges have always raised concerns for business owners [2]. Challenges that need to be thoroughly investigated because neglecting them can lead to irreparable damage. The supply chain is the core business cycle, so optimizing its processes can have a direct impact on business growth. Increasing the available data in business processes can make decision making in different sectors easier provided that there are fundamental solutions for the proper use of the data and appropriate operations for the proper analysis of data. Integrating of IoT digital technologies into supply chains requires a standard architecture to efficiently managing the complexities and resources [3].

Digital supply chains are exposing new types of cyber risks to the digital economy. The impact of IoT technologies on supply chain cyber risk has rarely been discussed in the academic literature, and the digital economy currently lacks clarity on the individual levels of the strategic, practical and operational challenges of IoT digital technologies in the supply chain. For this reason, in this study, it has been attempted to investigate the cyber risks that will arise from the use of IoT in the supply chain by examining the literature on the subject as well as examining the supply chain of the fast-moving consumer goods (FMCG) industry (specifically the food and pharmaceutical industries) and using expert opinions. Then, by a fuzzy ranking method using Mikhailov [4] non-linear modeling method based on the analytic hierarchy process (AHP) method, the importance of each cyber risk is examined.

In the first part, the literature review of the subject is examined in two categories: IoT and IoT based supply chain. In the second part, the cyber risks of the smart supply chain are analyzed with emphasis on the supply chain of FMCG companies and then by introducing the nonlinear fuzzy ranking method, the weight and rank of each cyber risk will be obtained. Finally, the results will be examined.

2. Literature Review

In this section, we review the literature on IoT and its applications and research, and in the second section, we review the literature on an IoT supply chain that forms the basis of this research.

2.1. Internet of Things (IoT)

The IoT is a network in which every physical object is identified by a tag and interacts with other objects. This communication can be controlled and managed using technologies available on smartphones and tablets [5]. Using IoT technology, goods can have more advantages than electronic IDs [6]. Using IoT, as one of the largest sources of big data generation, has many benefits for smart living as well as smart businesses [7]. These benefits include improving operational processes, creating value, reducing costs and minimizing risk as a result of the transparency, interoperability, adaptability, scalability and flexibility created by the IoT [8]. In the IoT pattern, many of the objects around us fall into one form or other forms in the networks.

Radio frequency identification (RFID) and sensor network technologies are increasing to meet this new challenge, and information and communication systems are inadvertently embedded in our surroundings. This generates huge amounts of data that these data should be stored, processed and presented in integrated and interpretable mode [9]. Cloud computing can provide the virtual infrastructure for such computing, with the ability to integrate monitoring devices, storage analytics, formatting, and customer delivery at the same time [10].

The cost-based model that cloud computing offers enables complete software and hardware services for businesses and users to access on-demand applications from anywhere. Smart connectivity with existing networks and comprehensive computing using network resources is an essential part of the IoT. However, for the successful emergence of IoT prospects, there is a need for computation beyond the computing and mobile scenarios that use smart and portable phones and it evolves in the interconnectedness of everyday objects and the current intelligence in our environment [11]. Given the importance of this technology and the growing use of this technology and its capabilities, much research has been done to date. For example, Akyildiz et al. [12] investigated the use of IoT in bus transportation systems. Kelly et al. [13] investigated the effective implementation of the IoT to monitor orderly internal conditions through a low-cost versatile sensing system. Huh et al. [14] evaluated the management of IoT tools using blockchain technology. Much research has also focused on the connection between IoT and the creation of smart cities. The technologies used to make cities smart are one of the most common applications of IoT [15 - 18]. Other applications of IoT, which are of great interest to researchers, include the study of this technology in the healthcare industry [15 - 18]. Much research has also focused on the development of IoT and its many applications in business development and business intelligence [19, 20]. In the following, we will explore further the use of IoT in the development and optimization of the supply chain.

2.2. IoT-based Supply Chain

The emergence of the Internet of Things and information technology has changed many concepts that smart business and therefore smart supply chain is one of them. As a result, many companies and organizations use information and communication technology to increase efficiency, reduce costs, and improve product quality [21]. A smart supply chain based on distributed and independent information

infrastructure comprises thousands of sources of information, in which different tools and capabilities are interconnected, using IoT or other similar technologies [22]. IoT is closely linked to big data analytics and it extremely permeates many areas to optimize energy efficiency and reduce environmental damaging effects. This is mainly related to the efficient use of natural resources, the intelligent management of infrastructure and facilities and the upgrading of environmental protection services. Likewise, big data and IoT applications have a great impact on facilitating and improving the sustainable development process of the environment [23].

Today, the emergence of topics such as smart businesses or business intelligence with the use of big data production technology and the collection, storage, processing and maintenance of this data has given rise to new concepts such as the smart supply chain. In the context of a smart and sustainable supply chain, the volume of data production is growing rapidly and a large amount of information in various areas of the supply chain, such as raw material supplying and relation with supplier, material delivery to production sites, production and manufacturing, and facilities related to production planning and ultimately regular distribution in real-time and communication with retailers and end customers are available. This data is so valuable that it can be used in collaboration with supply chain planners and decision-makers and IT professionals to promote environmental sustainability.

IoT technologies include a variety of sensors, data processing systems, wireless communication networks, and system activators in the physical environment [24]. Therefore, the term sustainable supply chain is a supply chain that describes the widespread development of advanced ICTs and their widespread use in various supply chain systems by utilizing secure, sustainable and efficient control tools, economic and social outcomes. Various researches have been carried out on the relationship between supply chain and its intelligentization using IoT. Many studies have examined the Radio-frequency identification (RFID) and their relationship to supplying and distribution systems [25 - 27]. Other research has examined the issue of manufacturing and building smart factories with the possibility of energy storage and process control to create sustainability for a healthier environment [28, 29]. Table (1) lists some of the research that has been done on the relationship between IoT and supply chain.

Table 1. Some IoT-based supply chain research.

Research subject	**Reference**
Manufacturing and smart factories	
Comprehensive production	Chen and Tsai [34]
Big data analysis for IoT-based production	Dai et al. [35]
Intelligent design and production control	Zawadzki and Żywicki [36]
IoT-based production of cloud computing	Wang et al. [37]
Production planning and scheduling	
IoT-based supply chain performance evaluation systems	Hwang et al. [38]
Real-time scheduling	Ivanov et al. [39]
Big data analytics for RFID logistics data	Zhong et al. [40]
Active maintenance	
Forecasting using data mining and intelligent algorithms	Kwon et al. [41]
IoT-based preventive maintenance for fleet management	Killeen et al. [42]
Maintenance in digital manufacturing	Bokrantz et al. [43]
Quality beyond factory	
Smart things and quality management functions	Putnik et al. [44]
Quality Management in Product Recovery Using IoT	Ondemir and Gupta [45]
Information management for supply chain quality management	Xu [46]
Sustainability	
IoT empowerment in the green supply chain	Chen et al. [47]
Sustainable Production Opportunities Using IoT-Based Supply Chain	Kamble et al. [48]

3. Cyber Risks of IoT-based Supply Chain

Risks are always around us, and governments, businesses, and individuals participate in risk-based decision-making every day. IoT systems include interoperability across multiple categories of physical-cyber systems, integration of technologies related to business smart networks, intelligent transportation, smart supply chain and smart manufacturing. Such new technologies are associated with new types of risks therefore the methods for predicting and managing these risks are specially designed [30]. Therefore, to safeguard IoT deployment, while also benefiting from its economic value, it is necessary to systematically consider multiple risk factors. Because cyberattacks occur more and more frequently and they are increasingly targeting IoT devices [31].

As cyberattack levels and capabilities continue to grow, the intensity of IoT attacks can be much greater than what has been observed to date. Therefore, one of the most important concerns for government policy as well as private sector business strategies regarding IoT products, platforms and services will be the adequacy of cyber security measures and techniques to minimize cyber risk [32]. Answering this concern is very important and the need to consider these risks. Because IoT capabilities create new types of cyber risks, they are not anticipated in the existing cyber risk assessment standards [33]. Risk assessment requires a thorough analysis of the data compatibility and capabilities of the network providers and data owners to develop, deploy, and cost-effective cyber security for important infrastructure.

In this study, to investigate cyber risks of supply chain based on IoT, supply chain of FMCG companies was selected as a case study. These companies have products that make up a large part of people's daily needs. Much of the cost of households is spent on buying these products. Given the importance and applicability of these industries, we have used the opinions of experts in the supply chain and information technology sectors in this study. Since IoT is one of the most important sources of big data, therefore, it is necessary to identify the sources of data generation in this chain to investigate cyber risks. Figure (1) shows the most important big data sources for the FMCG supply chain [49]. The scope of IoT activities is in the supply, production and distribution of products.

Information is collected and maintained via IoT systems and processed on cloud computing systems to be used to supply chain intelligence. Data are collected at each entry in the supply chain domain using computers, smartphones, tablets and a variety of sensors as IoT tools. The data are then processed using powerful processing systems and complete analyzes are made to make decisions as to the output of the smart supply chain system. Each of the IoT tools due to interactions in different parts of the supply chain can cause cyber breaches and threats to the supply chain. Given the interactive space in many parts of the supply chain, especially relationships with suppliers as well as customers, privacy is always an important issue. So there will be a lot of threatening space and cyberattacks. Distribution scheduling issues, especially for perishable products, are also critical issues in the FMCG supply chain, as disruptions to proper scheduling and distribution, problems with optimal routing, and the choice of high-traffic routes to distribute their products can pose a serious risk to supply and distribution as well as optimization of supply chain activities. According to the supply chain of FMCG companies, as well as the ways of entering big data and reviewing the literature of the subject and opinions of the active experts, cyber supply chain risks were identified in three areas of supply, production and distribution (Table 2).

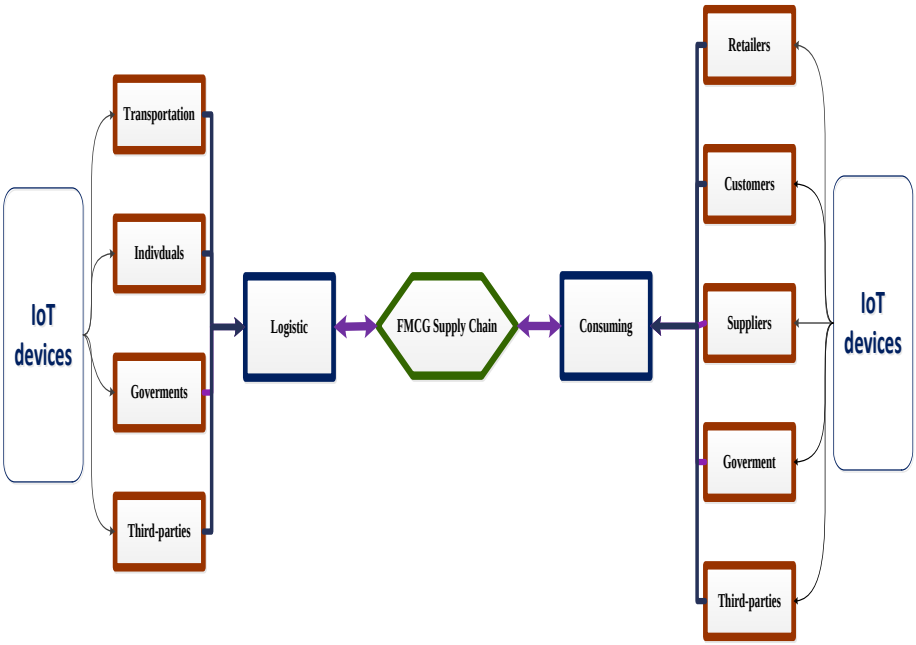

Fig. 1. Big data sources in the FMCG industry supply chain

Table 2. Cyber risks for the IoT supply chain

Area	Cyber risks	Code
Supply	Lack of security and privacy program interacting with suppliers	W1
	Disorder in transportation and delivery	W2
Production	Insufficient monitoring of devices and systems to detect security incidents	W3
	Lack of security in product design and ecosystem	W4
	Disorders in identifying and treating the risks of products	W5
	Lack of adequate security awareness and training for engineers	W6
Distribution and sales	Failure to implement privacy risk management in interaction with customers	W7
	Disorder of product inventory checking	W8
	Disruption of environment diagnostic programs and traffic	W9
	Interference with schedules for distribution and sales	W10

Based on the information in Table (2), we can conclude that one of the most important concerns for interacting with suppliers of goods and services as well as customers is privacy. By using electronic tools and receiving information from suppliers and extensively working communications through smartphones and tablets, huge amounts of personal and financial information can be shared, providing security for these sectors can be one of the most important challenges and concerns. Therefore, understanding the cyber risks in businesses that are smartened by the IoT can be a factor in creating organizational peace and thus increasing efficiency.

4. Methodology

The research methodology used in this research is a survey type and in terms of purpose type, it is applicable because it seeks to apply a decision-making method to rank cyber risks based on the IoT-based supply chain. Much of the information in the current study was collected by sending and completing questionnaires by experts of the field under study. The scope of research is some of the

FMCG industries (in particular food and pharmaceutical companies). In the present survey, opinions of 35 experts in the supply chain of FMCG companies were utilized.

The network structure of the problem was obtained through library review and literature review as well as interviews with experts and then verified using experts' opinions. To ensure consistency of the questionnaires, the responses of the experts have been monitored visually. In summary, the evaluation framework for this research is summarized below.

Identifying cyber risks in the IoT-based supply chain. To achieve this goal, using library studies and literature, the cyber risks and threats caused by the use of IoT in the supply chain were investigated and then the risks were refined validated by experts.

Creating a hierarchical structure. The hierarchical structure of cyber risks was created for the IoT-based supply chain using the levels of goals, criteria and alternatives. This structure is shown in Table (2). The purpose of this structure is to investigate the cyber risks of the supply chain in terms of supply, production and distribution.

Creating fuzzy judgment matrices. To analyze and rank the cyber risks in the smart supply chain, fuzzy pairwise comparison matrices are used based on experts' opinions by applying the AHP method. The linguistic criteria for the fuzzy pairwise comparisons used in this study are shown in Table (3). These scales are based on fuzzy triangular numbers.

Designing and solving a fuzzy nonlinear mathematical model: To rank cyber risks in the IoT supply chain, a non-linear mathematical ranking method, based on fuzzy hierarchical analysis, is employed.

In this study, a fuzzy ranking method is used based on hierarchical analysis, which was first proposed by Mikhailov [4]. In this method, the fuzzy pairwise comparisons matrix is first derived from triangular numbers and linguistic criteria (Table 3).

Table 3. Linguistic scales for pairwise comparisons and their fuzzy equivalents

Fuzzy scales	Linguistic values
Very Low	(1,2,3)
Low	(2,3,4)
Medium	(3,4,5)
High	(4,5,6)
Very high	(5,6,7)

These values are then used to rank the criteria using fuzzy nonlinear mathematical modeling according to the following relation.

$$
\begin{aligned}
&\text{Max } \lambda \\
&\text{s.t.} \\
&(m_{ij} - l_{ij})\lambda w_j - w_i + l_{ij} w_j \le 0 \\
&(u_{ij} - m_{ij})\lambda w_j + w_i - u_{ij} w_j \le 0 \\
&\sum_{k=1}^{n} w_k = 1 \\
&w_k > 0 \; ; \; k = 1,2,...,n \; ; \; i = 1,2,...,n-1 \; ; \\
&\qquad j = 2,3,...,n \; ; \; j > i
\end{aligned}
\qquad (1)
$$

where the values of the fuzzy triangular numbers obtained from the pairwise comparisons matrix are substituted and then the created model can be solved. Since the model is nonlinear, it is not possible to be solved using simple mathematical programming methods. Therefore, software, such as GAMS or LINGO can be applied to solve the model created. In the present study, LINGO software is utilized to solve models based on pairwise comparisons matrix.

After solving the model, the positive value obtained indicates that all the weights are completely true to the initial judgments, but if the index is negative, it can be found that the fuzzy judgments are not fully consistent or in other words, they are incompatible.

5. Research Finding

The main phases of assessing and ranking cyber risks in the smart supply chain can be divided into two general sections. In the first phase, expert opinions are extracted and merged using fuzzy questionnaires, as demonstrated by Tables (4) to (7). Then, using the nonlinear mathematical model presented in this study, the risks are ranked as illustrated in Tables 8 to 10. By incorporating the data from the pairwise comparisons tables obtained from the integration of expert opinions, fuzzy nonlinear mathematical models are formed and the resulting models are solved using LINGO software. As a result, the weight and ranking of each of the cyber risks are obtained in the areas of supply, production and distribution as presented in Tables (8) to (10).

Table 4. Fuzzy pairwise comparisons based on integration of expert opinions for general supply chain areas

	Supply			Production			Distribution		
	A1			A2			A3		
A1	-	-	-	-	-	-	-	-	-
A2	3.1	3	7	-	-	-	-	-	-
A3	3	3.1	5.6	2	2.5	2.5	-	-	-

Table 5. Fuzzy pairwise comparisons based on integration of expert opinions for supply area

	W1			W2		
W1	-	-	-	-	-	-
W2	3.1	4.3	6.1	-	-	-

Table 6. Fuzzy pairwise comparisons based on integration of expert opinions for production area

	W3			W4			W5			W6		
W3	-	-	-	-	-	-	-	-	-	-	-	-
W4	4.5	3.3	6.1	-	-	-	-	-	-	-	-	-
W5	4.5	3	4.1	4.5	3	4	-	-	-	-	-	-
W6	3.1	3.25	6	3	4.1	4.1	2	2.3	2.6	-	-	-

Table 7. Fuzzy pairwise comparisons based on integration of expert opinions for distribution area

	W7			W8			W9			W10		
W7	-	-	-	-	-	-	-	-	-	-	-	-
W8	5.1	4.2	6	-	-	-	-	-	-	-	-	-
W9	2.25	3.1	4.3	2.1	2.1	3.2	-	-	-	-	-	-
W10	2.5	4	4.4	3	6.1	3	2	2.1	3.2	-	-	-

Table 8. The weight and ranking of each cyber risk for the supply area

Cyber risk	Code	Weight	Rank
Lack of security and privacy program interacting with suppliers	W1	0.612734	1
Disorder in transportation and delivery	W2	0.387266	2

Table 9. Weight and ranking of each cyber risk for the production area

Cyber risk	Code	Weight	Rank
Insufficient monitoring of devices and systems to detect security incidents	W3	0.273004	2
Lack of security in product design and ecosystem	W4	0.309915	1
Disorders in identifying and treating the risks of products	W5	0.240076	3
Lack of adequate security awareness and training for engineers	W6	0.177004	4

Table 10. Weight and ranking of each cyber risk for the distributions area

Cyber risk	Code	Weight	Rank
Failure to implement privacy risk management in interaction with customers	W7	0.309915	1
Disorder of product inventory checking	W8	0.211259	4
Disruption of environment diagnostic programs and traffic	W9	0.228911	3
Interference with schedules for distribution and sales	W10	0.249915	2

By investigating the weights achieved from mathematical modeling, the extent of cyber risks in the IoT supply chain can be found. Subsequently, by normalizing the obtained weights, the overall ranking of cyber risks in the smart supply chain can be achieved. This ranking is shown in Figure (2), which indicates that privacy in the interaction with suppliers and customers is the most important issue among the cyber risks of the smart supply chain. Then, all the weights are normalized and the final ranking is obtained.

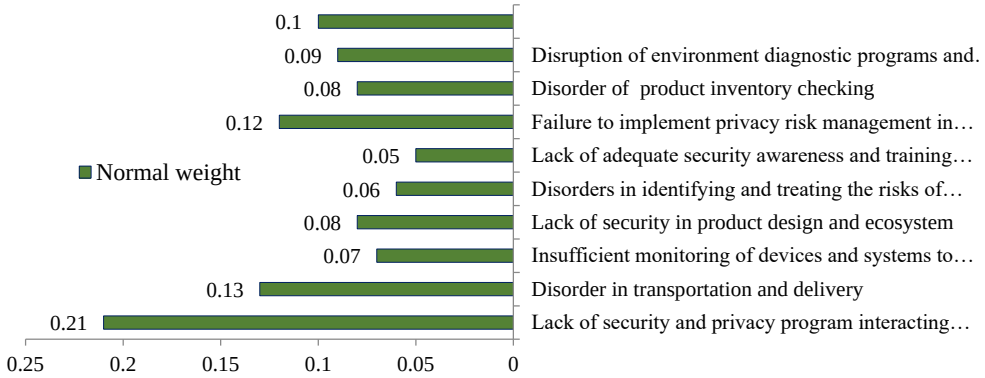

Fig. 2. Normal weight of cyber risks in the smart supply chain

Figure (2) shows the normalized weights that illustrate the importance of cyber risks in the IoT supply chain.

6. Conclusion

Nowadays, the advent of IoT technology and the wide range of applications using IoT, businesses are also looking to take the advantages of this technology. Meanwhile, the combination of the IoT concept and the supply chain as a business lifecycle has made many researchers examine the various dimensions

of this integration. Since the supply chain encompasses a large part of the activity of an organization from raw materials to distribution, a good understanding of the applications of the IoT technology can facilitate the optimization of a variety of processes in the organization. IoT can be one of the most important data producers, which can help in making real-time decisions in the organization if analyzed and processed properly. At the same time, since this technology is intertwined with the Internet, its use can always face challenges and concerns. The present study attempts to identify and understand the cyber risks that an IoT-based supply chain can deal with by identifying the sources of big data production in the supply chain of FMCG industries (food and pharmaceutical industries), as the case study. To investigate the significance of each of these risks, a fuzzy ranking method using nonlinear mathematical modeling was used. The research results indicate that privacy in interaction with suppliers and customers is one of the most important cyber risks of the smart supply chain in these companies.

References

[1] Nozari, H., Fallah, M., Kazemipoor, H., & Najafi, S. E. (2021). Big data analysis of IoT-based supply chain management considering FMCG industries. Бизнес-информатика, 15(1 (eng)). DOI: 10.17323/2587-814X.2021.1.78.96

[2] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in industry, 101, 1-12. https://doi.org/10.1016/j.compind.2018.04.015

[3] Nozari, H., Fallah, M., & Szmelter-Jarosz, A. (2021). A conceptual framework of green smart IoT-based supply chain management. International Journal of Research in Industrial Engineering, 10(1), 22-34. DOI: 10.22105/riej.2021.274859.1189

[4] Mikhailov, L. (2003). Deriving priorities from fuzzy pairwise comparison judgements. Fuzzy sets and systems, 134(3), 365-385. https://doi.org/10.1016/S0165-0114(02)00383-4

[5] Ashton, K. (2009). That 'internet of things' thing. RFID journal, 22(7), 97-114.

[6] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[7] Nouri, F., & Ghahremani Nahr, J. (2019). Structural-interpretative Patterns of Factors Affecting the Sustainable Development of Agricultural Production Cooperatives (Case Study: East Azerbaijan Province), Journal of Agricultural Economics and Development, 33(3), pp. 281-297.

[8] Sinha, B. B., & Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. Future Generation Computer Systems, 126, 169-184. https://doi.org/10.1016/j.future.2021.08.006

[9] Alsalibi, A. I., Shambour, M. K. Y., Abu-Hashem, M. A., Shehab, M., Shambour, Q., & Muqat, R. (2022). Nonvolatile Memory-Based Internet of Things: A Survey. In Artificial Intelligence-based Internet of Things Systems (pp. 285-304). Springer, Cham.

[10] Zahedi, M., & Nahr, J. (2020). Designing a hub covering location problem under uncertainty conditions. Management Science Letters, 9(3), 477-500. DOI: **10.5267/j.dsl.2020.2.002**

[11] Al-Turjman, F. (2019). 5G-enabled devices and smart-spaces in social-IoT: an overview. Future Generation Computer Systems, 92, 732-744. https://doi.org/10.1016/j.future.2017.11.035

[12] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks, 38(4), 393-422. https://doi.org/10.1016/S1389-1286(01)00302-4

[13] Ghahremani Nahr, J., Zahedi, M. (2021). Modeling of the supply chain of cooperative game between two tiers of retailer and manufacturer under conditions of uncertainty. *International Journal of Research in Industrial Engineering*, 10(2), 95-116. DOI: 10.22105/riej.2021.276520.1190

[14] Nozari, H., Fallah, M., Szmelter-Jarosz, A., & Krzemiński, M. (2021). Analysis of security criteria for IoT-based supply chain: a case study of FMCG industries. Central European Management Journal, 29(4).

[15] Nozari, H., & Sadeghi, M. E. (2020). Identifying the challenges facing the telecommuting plan and providing solutions for its effective implementation-a case study of the ministry of industry, mines and trade.

[16] Arogia Victor Paul, M., Anil Sagar, T., Venkatesan, S., & Gupta, A. K. (2019). Impact of mobility in IoT devices for healthcare. In Digital business (pp. 243-261). Springer, Cham.

[17] Nozari, H., Szmelter-Jarosz, A., & Ghahremani-Nahr, J. (2021). The Ideas of Sustainable and Green Marketing Based on the Internet of Everything—The Case of the Dairy Industry. Future Internet, 13(10), 266. https://doi.org/10.3390/fi13100266

[18] Shamsollahi, M., Badiee, A., & Ghazanfari, M. (2019). Using combined descriptive and predictive methods of data mining for coronary artery disease prediction: a case study approach. Journal of AI and Data Mining, 7(1), 47-58. DOI: 10.22044/jadm.2017.4992.1599

[19] Nozari, H., & Sadeghi, M. E. (2021). Artificial intelligence and Machine Learning for Real-world problems (A survey). International Journal of Innovation in Engineering, 1(3), 38-47.

[20] Viriyasitavat, W., Da Xu, L., Bi, Z., & Pungpapong, V. (2019). Blockchain and internet of things for modern business process in digital economy—the state of the art. IEEE Transactions on Computational Social Systems, 6(6), 1420-1432. DOI: 10.1109/TCSS.2019.2919325

[21] Nahr, J. G., Nozari, H., & Sadeghi, M. E. (2021). Green supply chain based on artificial intelligence of things (AIoT). International Journal of Innovation in Management, Economics and Social Sciences, 1(2), 56-63. https://doi.org/10.52547/ijimes.1.2.56

[22] Singh, B., & Gupta, A. (2015). Recent trends in intelligent transportation systems: a review. Journal of Transport Literature, 9, 30-34.

[23] 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. https://doi.org/10.1016/j.scs.2017.12.034

[24] O'Donovan, P., Leahy, K., Bruton, K., & O'Sullivan, D. T. (2015). An industrial big data pipeline for data-driven analytics maintenance applications in large-scale smart manufacturing facilities. Journal of Big Data, 2(1), 1-26. https://doi.org/10.1186/s40537-015-0034-z

[25] Musa, A., & Dabo, A. A. A. (2016). A review of RFID in supply chain management: 2000–2015. Global Journal of Flexible Systems Management, 17(2), 189-228. https://doi.org/10.1007/s40171-016-0136-2

[26] Nativi, J. J., & Lee, S. (2012). Impact of RFID information-sharing strategies on a decentralized supply chain with reverse logistics operations. International Journal of Production Economics, 136(2), 366-377. https://doi.org/10.1016/j.ijpe.2011.12.024

[27] Ngai, E. W., Cheung, B. K., Lam, S. S., & Ng, C. T. (2014). RFID value in aircraft parts supply chains: A case study. International Journal of Production Economics, 147, 330-339. https://doi.org/10.1016/j.ijpe.2012.09.017

[28] Strozzi, F., Colicchia, C., Creazza, A., & Noè, C. (2017). Literature review on the 'Smart Factory'concept using bibliometric tools. International Journal of Production Research, 55(22), 6572-6591. https://doi.org/10.1080/00207543.2017.1326643

[29] Tao, F., Zuo, Y., Da Xu, L., & Zhang, L. (2014). IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE transactions on industrial informatics, 10(2), 1547-1557. DOI: 10.1109/TII.2014.2306397

[30] Orojloo, H., & Azgomi, M. A. (2017). A game-theoretic approach to model and quantify the security of cyber-physical systems. Computers in Industry, 88, 44-57. https://doi.org/10.1016/j.compind.2017.03.007

[31] Hamidi, H. (2016). Safe use of the internet of things for privacy enhancing. Journal of Information Systems and Telecommunication, 4(3), 145-151.

[32] Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R., & Huth, M. (2018). Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. DOI: 10.1049/cp.2018.0003

[33] Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of network and computer applications, 42, 120-134. https://doi.org/10.1016/j.jnca.2014.01.014

[34] Tsai, Y. S., Chen, R. S., Chen, Y. C., & Yeh, C. P. (2013). An RFID-based manufacture process control and supply chain management in the semiconductor industry. International journal of information technology and management, 12(1-2), 85-105.

[35] Dai, H. N., Wang, H., Xu, G., Wan, J., & Imran, M. (2020). Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies. Enterprise Information Systems, 14(9-10), 1279-1303. https://doi.org/10.1080/17517575.2019.1633689

[36] Zawadzki, P., & Żywicki, K. (2016). Smart product design and production control for effective mass customization in the Industry 4.0 concept. Management and production engineering review.

[37] Wang, Y., Lin, Y., Zhong, R. Y., & Xu, X. (2019). IoT-enabled cloud-based additive manufacturing platform to support rapid product development. International Journal of Production Research, 57(12), 3975-3991. https://doi.org/10.1080/00207543.2018.1516905

[38] Lee, M., Hwang, J., & Yoe, H. (2013, December). Agricultural production system based on IoT. In 2013 IEEE 16Th international conference on computational science and engineering (pp. 833-837). IEEE. DOI: 10.1109/CSE.2013.126

[39] Ivanov, D., Sokolov, B., Solovyeva, I., Dolgui, A., & Jie, F. (2016). Dynamic recovery policies for time-critical supply chains under conditions of ripple effect. International Journal of Production Research, 54(23), 7245-7258. https://doi.org/10.1080/00207543.2016.1161253

[40] Zhong, R. Y., Lan, S., Xu, C., Dai, Q., & Huang, G. Q. (2016). Visualization of RFID-enabled shopfloor logistics Big Data in Cloud Manufacturing. The International Journal of Advanced Manufacturing Technology, 84(1), 5-16. https://doi.org/10.1007/s00170-015-7702-1

[41] Kwon, D., Hodkiewicz, M. R., Fan, J., Shibutani, T., & Pecht, M. G. (2016). IoT-based prognostics and systems health management for industrial applications. IEEE Access, 4, 3659-3670. DOI: 10.1109/ACCESS.2016.2587754

[42] Killeen, P., Ding, B., Kiringa, I., & Yeap, T. (2019). IoT-based predictive maintenance for fleet management. Procedia Computer Science, 151, 607-613. https://doi.org/10.1016/j.procs.2019.04.184

[43] Bokrantz, J., Skoogh, A., Berlin, C., & Stahre, J. (2017). Maintenance in digitalised manufacturing: Delphi-based scenarios for 2030. International Journal of Production Economics, 191, 154-169. https://doi.org/10.1016/j.ijpe.2017.06.010

[44] Ghahremani-Nahr, J., & Nozari, H. (2021). A Survey for Investigating Key Performance Indicators in Digital Marketing. International journal of Innovation in Marketing Elements, 1(1), 1-6.

[45] Ondemir, O., & Gupta, S. M. (2014). Quality management in product recovery using the Internet of Things: An optimization approach. Computers in Industry, 65(3), 491-504. https://doi.org/10.1016/j.compind.2013.11.006

[46] Xu, L. D. (2011). Information architecture for supply chain quality management. International Journal of Production Research, 49(1), 183-198. https://doi.org/10.1080/00207543.2010.508944

[47] Nahr, J. G., Bathaee, M., Mazloumzadeh, A., & Nozari, H. (2021). Cell Production System Design: A Literature Review. International Journal of Innovation in Management, Economics and Social Sciences, 1(1), 16-44. https://doi.org/10.52547/ijimes.1.1.16

[48] Kamble, S. S., Gunasekaran, A., & Gawankar, S. A. (2018). Sustainable Industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives. Process safety and environmental protection, 117, 408-425. https://doi.org/10.1016/j.psep.2018.05.009

[49] Nozari, H., Najafi, E., Fallah, M., & Hosseinzadeh Lotfi, F. (2019). Quantitative analysis of key performance indicators of green supply chain in FMCG industries using non-linear fuzzy method. Mathematics, 7(11), 1020. https://doi.org/10.3390/math7111020

[50] Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., ... & Pfisterer, D. (2014). SmartSantander: IoT experimentation over a smart city testbed. Computer Networks, 61, 217-238. https://doi.org/10.1016/j.bjp.2013.12.020

[51] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by internet of things. Transactions on emerging telecommunications technologies, 25(1), 81-93. https://doi.org/10.1002/ett.2704

[52] Liu, Y., Yang, C., Jiang, L., Xie, S., & Zhang, Y. (2019). Intelligent edge computing for IoT-based energy management in smart cities. IEEE network, 33(2), 111-117. DOI: 10.1109/MNET.2019.1800254

[53] Singh, A. K., Kumar, D., & Prakash, V. (2019, March). Importance and needs of IoT in developing smart cities. In Proceedings of 2nd international conference on advanced computing and software engineering (ICACSE).

[54] Ji, G., Hu, L., & Tan, K. H. (2017). A study on decision-making of food supply chain based on big data. Journal of Systems Science and Systems Engineering, 26(2), 183-198. https://doi.org/10.1007/s11518-016-5320-6

[55] Tavakkoli-Moghaddam, R., Ghahremani-Nahr, J., Samadi Parviznejad, P., Nozari, H., Najafi, E. (2021). Applications of Internet of Things in the Food Supply Chain: A Literature Review. Journal of Applied Research on Industrial Engineering, (), -. doi: 10.22105/jarie.2021.301205.1368.