INTERNET OF THINGS AND ITS CHALLENGES IN SUPPLY CHAIN MANAGEMENT: A ROUGH STRENGTH-RELATION ANALYSIS METHOD

Mahsa Pishdar, Fatemeh Ghasemzadeh, Jurgita Antucheviciene, Jonas Saparauskas

Introduction

Internet of Things (IOT) technology which turns out as a buzzword in the ICT contains elements such as biometrics, sensors and controlling data of the real world into the information technology platform (Mital et al., 2017). Research institutes predict its economic potential to be enormous and applicable in different industries such as healthcare, energy management, industrial automation, environmental management, traffic management, logistic and supply chain management (Kim & Kim, 2016).

IOT surly impacts businesses and changes logistics and supply chain management approaches. The research institute, Gartner, announced that a thirty-fold increase appears in Internet-connected physical devices by the year 2020 and this obviously changes the supply chain management specially in the way of obtaining information (Shankar, 2017).

These alternations show up more clearly in some special types of supply chains such as Fast Moving Consumer Goods (FMCG) supply chains. FMCGs are produced at low cost and in high circulations which are relatively quick corrupt. Marketing professionals believe that the consumers of FMCG industry are one of the most disloyal ones. These consumers usually make their decisions about purchasing a product in this industry based on subconscious and emotions and not their logics. This makes the FMCG industry as one of the most unstable and toughest industries for the gain of success (Woodside et al., 2012).

As a result, these supply chains need special systems to deal with perishable products, unforeseen supply variations and precise food safety and sustainability requirements. The needs are tangible in many other kinds of supply chains. IOT is a promising technology in conquering these challenges, since it makes simulation and optimization of processes possible using software systems instead of conducting physical experiments. It also can be used in the operational management of FMCG supply chains. Therefore, all kinds of supply chains can be controlled, planned and optimized remotely and in real-time via the IOT technology application (Verdouw et al., 2013; 2015).

These positive characteristics have made much talk about IOT. Although recent studies are mostly focused on IOT applications, they usually do not extend that research to the supply chain and only magnify specific IOT technology advantages. The number of studies that have considered obstacles and negative points of the IOT are also much less. However, IOT promises to bring new challenges and concerns in the format of technical, social or environmental matters in each kind of supply chain. Of course, none of these challenges is necessarily a reason to reject the IOT Technology, nor means that the IOT won't be a success or revolutionize technology. It means that its consequences are difficult to predict and the challenges of its application should be investigated as much as possible in order to be able to get use of this technology in a most suitable and effective way.

Most of these challenges are correlated to each other. For instance, lack of legislation framework causes security damages and harm users. These relations that are not sometimes easily observable make conditions worse and influence all partners through the whole supply chain. Decision making and trial evaluation laboratory (DEMATEL) is an

 DOI: 10.15240/tul/001/2018-2-014

applicable method that is used to explore interconnections of challenges, including supply chain management (Song et al., 2017; Debnath et al., 2017; Supeekit et al., 2016; Liou et al., 2016; Rajesh & Ravi, 2015; Pourahmad et al., 2015; Gandhi et al., 2015). However, this method is based on experts' opinions and it is obvious that expert knowledge is somehow imprecise and subjective. Their decision making process may contain inconsistency, since decision makers use the vague verbal judgments to make decisions (Song et al., 2017; Ebrahimnejad et al., 2017; Foroozesh et al., 2017). The point is that IOT application in supply chain management is an approach that is still in its growth stage. It is not unlikely that experts face imprecise information in their decision making process. Rough set theory that is introduced by Pawlak (1982) deals with such vagueness and inconsistent, inaccurate and incomplete information (Jian et al., 2011). Fuzzy generalisations of rough sets theory have been reviewed recently (Mardani et al., 2017).

The objective of this study is to find the critical IOT application challenges in supply chain management and their interrelationships in merit of a novel method of rough DEMATEL. In this way, IOT challenges interactions are explored and the strength of the interactions between these challenges are revealed considering the impression of decision makers' information. The cause and effect relationships between challenges are graphically depicted. Compared with the conventional group DEMATEL, this method is more accurate in discerning interactions between IOT application challenges without much prior information.

The structure of this paper is as follows: the first section contains a brief literature review of IOT and its application in supply chain management as well as methods for analyzing interaction of effective factors in applying IOT supply chain management. Research methodology and data analysis are explained in Section 2 and managerial insights are discussed afterwards in Section 3. Finally, conclusions of the paper, including suggestions for further research, are presented.

1. Literature Review

1.1 IOT and Its Application in Supply Chain Management

IOT is interpreted as a new concept which is officially introduced since 1990s. By the year 2013, IOT emerged as a system by use of multiple technologies including technologies raging from the automation of buildings and homes to complicated wireless systems. It is obvious that interaction of things generates value for both customers and businesses. IOT can promise new advantages in this domain (Saarikko et al., 2017).

Ownership of customer's data and its analysis procedure or the process of suitable legislative and technical frameworks creation to put more supervision over such a complicated environment should be under considerations while considering avoidance of applying unnecessary constraints to IOT market expansion (Fernandez-Gago et al., 2017).

There are also other important matters that show off easily. It should be determined that who has access to what kind of data. Governance, security and privacy aspects rise while pointing to ethical aspects. Governance sets the basis of each system manipulation and as a whole refers to five main aspects of openness, participation, accountability, effectiveness and coherence in order to set rules and processes of powers execution. The concept of governance have been already applied to the internet and organizations like IETF, ICANN, RIRs, ISOC, IEEE, IGF, W3C are working on deployment of this concept. However, extension of this effort to IOT with suitable control limits which can support decision making is essential too (IERC, 2015).

Another matter that can put IOT concept at risk is that many stakeholders have different positions and their orientation change over time. Each of them has special vision and specific role in deployment of IOT concept. This enhances environmental dynamics and makes the prediction of IOT application much more difficult considering also the technology revolution (Zarpelão et al., 2017; Fernandez-Gago et al., 2017). These matters put strategy making and scenario planning into troubles too, since companies are not familiar with the concept, its details and even the dynamics of its application (Verdouw et al., 2015). Such unconsciousness causes every single IOT device to present a potential challenge of jeopardizing the privacy of users and faces security issues with difficulty (Farahani et al., 2017).

Global data synchronization and global commerce initiative are recent trends that each

supply chain may face in order to improve international supply chains. IOT has its hopes and concerns in supply chain management in different functions ranging from inbound logistic to outbound operations too. The combination of mobile computing, immediate analysis of gathered data and cloud services which are shaped through IOT concept is changing how inbound and outbound logistics are conducted. One of the popular methods for delivery of goods is shaped by use of third party logistic (3PL) concept which can include any company participating in outsourcing for transferring goods. IOT helps this process to be done by consuming less time and money. Internet-connected trackers which can be interpreted as the next generation of RFID technology let companies pursue goods throughout their delivery veins. So, different sections of supply chain management can be fueled by IOT technology (Meola, 2016; Kees et al., 2015). However, such hopes bring challenges with them too as mentioned before.

1.2 Methods for Analyzing Interaction of Effective Factors in Applying IOT Supply Chain Management

Such challenges that mentioned previously make IOT concept to be discussed via industrial operations and manufacturing supply chain management perspective (Kees et al., 2015), and also from product and services supply chain management approach (Addo-Tenkorang & Helo, 2016). It is acknowledged now in practice and in research that these factors are interconnected (Hsu & Yeh, 2016; Fernandez-Gago et al., 2017).

Hsu and Yeh (2016) specified the key factors influencing IOT adoptions, considering especial situations in Taiwan's logistics industry. Their study ended in twelve factors in four dimensions of technology, organization, environment and security. They applied Decision-Making Trial and Evaluation Laboratory (DEMATEL) technique to specify the cause-effect relationships of these twelve factors. Yupeng et al. (2017) focused on intelligent medical terminals and consumers' adoption behavior. They specified ten factors classified into five dimensions of technical, security, contact, marketing and environment. They used a hybrid Multiple Attribute Decision-Making (MADM) model in order to clarify the relationships of these factors and their priorities of receiving attention. DEMATEL technique is used to build a cause-effect relationship map. Then, DEMATEL and Analytic Network Process (ANP) methods are combined to determine the influential weights and priorities. At last, VIse Kriterijumska Optimizacija I Kompromisno Resenje (VIKOR) method is applied to evaluate the existed gaps to conquer the consumers' needs for making sustainable improvements. Lu et al. (2013) also used this combination of techniques and focused on promoting RFID adoption in Taiwan's healthcare system which is a part of IOT technology. Meanwhile, Park and Shin (2017) threw a magnifying glass on security factors of the IOT services by integration of fuzzy DEMATEL and fuzzy ANP to reflect mutual interrelations among security factors and their priorities. Fernandez-Gago et al. (2017) got another approach and focused on the trust making in users and its dynamics which are created because of high interoperability of different matters in uncertain situation. A framework is developed to help scholars to include trust in IOT scenarios. Teixeira et al. (2017) put their considerations on securing IOT via distributed systems analysis. Distributed system is considered as an integrated body and introduced a novel algorithm to improve efficiency. Riahi Sfar et al. (2017) investigated security challenges in IOT application via a systematic and cognitive approach. They configured main actors in supply chain and determined security related matters such as trust and privacy and the role of each actor in the promotion of these factors. Krotov (2017) chose another perspective because of the importance of introducing new business opportunities to the entrepreneurs. Various factors are considered within the technological, physical, and socioeconomic dimensions. These factors are just depicted to show various opportunities and threads related to IOT.

As is obvious, IOT, its challenges and opportunities are somewhat investigated by various scholars. However, the previous studies often omit the requirement interactions while analyzing IOT application. Many of them also ignore flexible approaches to handle the subjective judgments of decision makers under vague environment. Some scholars apply fuzzy methods to deal with the subjective and vague evaluations, but these fuzzy methods need much information in advance about matters such as data distribution. Besides, many of the previous approaches do not provide graphical

causal and effect relationships among IOT challenges or advantages. Therefore, it is clear that developing a systematic method for evaluating and analyzing interactions among IOT challenges under vague environment is necessary.

2. Evaluation of IOT Application Challenges Based on Rough Group DEMATEL

2.1 IOT Application Challenges

Based on previous studies, it can be said that IOT application challenges has not received enough attention while the advantages of this new technology is taken into consideration. That is while the application of this technology brings different challenges. The situation becomes worse when it comes to especial domains such as supply chain management. The supply chain is either a type of service or a product one contains various actors. Information flows in different parts of supply chain prone to security hazards and this is just one of the miscellaneous challenges that should be in the center of attention in supply chain management. Sixteen IOT application challenge in supply chain management are obtained in Tab. 1 with a systematic and comprehensive literature review of IOT challenge, risk management and supply chain management and also consulting experts.

Tab. 1: IOT challenges in supply chain management (Part 1)

Challenges	Description	Previous Studies
Operational Challenges		
Ch1: Difficulty of consequences prediction	IOT is a revolutionizing technology and it is not exactly determined that how and where it can be used. So the consequences of its application are unpredictable.	Zarpelão et al., 2017; Banafa, 2016; Dutton, 2014
Ch2: Lack of strategy and scenario planning in IOT	Many companies haven't yet defined their strategies about Internet of Things and they really do not know how the generated information can be used for controlling at a supply chain level.	Fernandez-Gago et al., 2017; Verdouw et al., 2015
Ch3: Storage issues	The amount of information generated by smart devices goes up and this causes difficulty in what kind of information should be stored and for how long. This will increase the energy demands.	Banafa, 2016; Gill et al., 2016
Ch4: Lack of security	Lack of security seems trivial once the IOT is applied.	Fernandez-Gago et al., 2017; Zarpelão, et al., 2017; Dutton, 2014
Ch5: Lack of privacy	The IOT makes unique challenges that goes beyond the data privacy and contains voice recognition or vision features of customers.	Fernandez-Gago et al., 2017; Zarpelão et al., 2017; Kim & Kim; 2016
Integration Challenges		
Ch6: Scalability and Interoperability	The need for highly specialized and highly customized solutions makes IOT difficult to scale through the supply chain. It is challenging to make meaningful connections between devices and make processes open to foster the interoperability and reutilization.	Atzori et al., 2017; Zarpelão et al., 2017; Fernandez-Gago et al., 2017
Ch7: Financial matters	Cost sharing while enabling supply chain with IOT can be challenging. The value of the data or service that can be derived from an IOT deployment will not always cover the expense.	Kim & Kim; 2016; Dutton, 2014

Tab. 1: IOT challenges in supply chain management (Part 2)

Challenges	Description	Previous Studies
Ch8: The need for open standards	IOT is likely to be built with open source software. However, universal standards and protocols lag behind the development of smart technology.	Kim & Kim; 2016
Ch9: New business model	Business processes of different parts of supply chain such as suppliers, manufactures and distributors should fit into the digital network and adapting to the new business model.	Lee, 2017; Kim & Kim; 2016; Verdouw et al., 2015
Ch10: Responsibility sharing	It must become clear who is responsible if mistakes happen in IOT enabled supply chains as like as personal health related processes.	Atzori et al., 2017
Environmental Challenges		
Ch11: Energy demands	The use of smart devices would be increased so fast and this means the more need to energy. Meeting the demand even with improved batteries and green sources like solar and wind will not be easy too.	Atzori et al., 2017
Ch12: Waste disposal	The amount of e-waste such as the disposal of computers, phones, and peripherals will be grown up by the extension of IOT devises use.	Kim & Kim; 2016
Social Challenges		
Ch 13: Legal framework for IOT governance	Lack of analysis of the IOT governance issues such as legitimacy, transparency and accountability seems to be challenges creator	Atzori et al., 2017; IERC, 2015; Weber, 2013
Ch14: Trust creation and user acceptance	IOT makes things to interact with each other often in uncertain conditions. Trust creation among stakeholders can be a challenge because of this. People who do not have a clue about IOT operations should become able to trust it.	Fernandez-Gago et al., 2017; Mital et al., 2017; Kim & Kim, 2016
Ch15: Dynamic environment	The intrusive behavior and benign behavior of users, systems, or network change over time.	Zarpelão et al., 2017; Fernandez-Gago et al., 2017

Source: own

Although an investigation of such challenges in IOT-based supply chain plays an important role in the efficiency improvement, the previous methodologies have not considered their mutual relations in a graphical format. Besides, the vagueness and subjectivity that decision makers face are not considered in analysis. That is why it seems necessary to evaluate mutual relations of challenges in a more systematic manner considering the existed vagueness and subjectivity. In this paper, rough theory is combined with group DEMATEL to take use of advantage of DEMATEL in conquering different experts' opinions and capability of rough theory in manipulating vagueness and subjectivity. The steps of rough DEMATEL are described as following.

2.2 Group Rough DEMATEL Application

Although these challenges are self-presented in each kind of supply chain, the experts are chosen from FMCG industry to evaluate the relationships between these challenges. FMCG consumers show less loyalty and the industry is facing much dynamic business environment. IOT is changing established business models and representing both challenges and opportunities for the FMCG supply chains. That is why the experts are selected from this industry. 13 managers in supply chain

Tab. 2: Linguistic terms for rating mutual relations of IOT application challenges

Linguistic term	Corresponding score
No strength	0
Low strength	1
Medium Strength	2
High strength	3
Very high strength	4

Source: own

management are asked to announce their opinions about IOT application challenges via linguistic terms as is shown in Tab. 2. Each expert's crisp direct-relation matrix is specified.

By taking average of opinions, the total crisp direct relation matrix is obtained as follows where m is the number of experts and n is the number of elements:

$$R = \begin{bmatrix} 0 & r_{12} & \text{K} & r_{1m} \\ r_{21} & 0 & \text{K} & r_{2m} \\ \text{M} & \text{M} & \text{O} & \text{M} \\ r_{n1} & r_{n2} & \Lambda & 0 \end{bmatrix}; \quad r_{ij} = \left\{ r_{ij}^1, r_{ij}^2, ..., r_{ij}^m \right\}.$$

Now, the crisp group direct matrix can be transformed to rough group direct matrix. In this regard, $r_{ij} = \{r^1_{ij}, r^2_{ij}, ..., r^m_{ij}\}$ should be ordered ascending. Then an interval should be obtained from each crisp judgment. r^k_{ij} upper and lower limits are specified as follows:

$$UL\left(r_{ij}^k\right) = \frac{\sum_{m=1}^{N_{ij}^U} y_{ij}}{N_{ij}^U}, \tag{1}$$

$$LL\left(r_{ij}^k\right) = \frac{\sum_{m=1}^{N_{ij}^L} x_{ij}}{N_{ij}^L}, \tag{2}$$

N^U_{ij} and N^L_{ij} are the number of elements used in upper limit and lower limit determination of r^k_{ij} (Zhai et al., 2009). In this way, all crisp judgments are transformed into rough numbers $\left[UL(r_{ij}^k) \quad LL(r_{ij}^k)\right] = \left[r_{ij}^{Lk} \quad r_{ij}^{Uk}\right]$.

The average of these rough numbers should be specified by use of arithmetic means of upper limit and lower limit of r^k_{ij}:

$$r_{ij}^L = \frac{\sum_{k=1}^{m} r_{ij}^{Lk}}{m}, \tag{3}$$

$$r_{ij}^U = \frac{\sum_{k=1}^{m} r_{ij}^{Uk}}{m}. \tag{4}$$

The rough group direct relation matrix is constituted of these rough interval numbers:

$$R_{Rough} = \begin{bmatrix} [0 \quad 0] & \left[r_{12}^L \quad r_{12}^U\right] & \text{K} & \left[r_{1m}^L \quad r_{1m}^U\right] \\ \left[r_{21}^L \quad r_{21}^U\right] & [0 \quad 0] & \text{K} & \left[r_{2m}^L \quad r_{2m}^U\right] \\ \text{M} & \text{M} & \text{O} & \text{M} \\ \left[r_{n1}^L \quad r_{n1}^U\right] & \left[r_{n2}^L \quad r_{n2}^U\right] & \Lambda & [0 \quad 0] \end{bmatrix}. \tag{5}$$

The rough group direct relation matrix of the challenges in this study is constructed as Tab. 3 via considering opinions of experts in FMCG supply chain management.

The rough group direct relation matrix should be normalized. In this regard, all the values of rough group direct relation matrix are divided by the maximum value of upper limits:

$$R^N{}_{Rough} = \begin{bmatrix} [0 \quad 0] & \left[\frac{r_{12}^L}{\vartheta} \quad \frac{r_{12}^U}{\vartheta}\right] & \text{K} & \left[\frac{r_{1m}^L}{\vartheta} \quad \frac{r_{1m}^U}{\vartheta}\right] \\ \left[\frac{r_{21}^L}{\vartheta}, \frac{r_{21}^U}{\vartheta}\right] & [0 \quad 0] & \text{K} & \left[\frac{r_{2m}^L}{\vartheta} \quad \frac{r_{2m}^U}{\vartheta}\right] \\ \text{M} & \text{M} & \text{O} & \text{M} \\ \left[\frac{r_{n1}^L}{\vartheta} \quad \frac{r_{n1}^U}{\vartheta}\right] & \left[\frac{r_{n2}^L}{\vartheta} \quad \frac{r_{n2}^U}{\vartheta}\right] & \Lambda & [0 \quad 0] \end{bmatrix} \tag{6}$$

where $\vartheta = \max_{1 \le i \le n} \left(\sum_{j=1}^{n} r_j^U \right)$.

Theta value in this study is 52.04 and the normalized rough group direct relation matrix is specified via equation 6 as Tab. 4.

The rough total-relation matrix T is gained as follows and by taking aid of unit matrix I:

$$T = \begin{bmatrix} t_{ij}^{L} & t_{ij}^{U} \end{bmatrix}_{n*n} = R^{N}{}_{Rough}(I - R^{N}{}_{Rough})^{-1} \quad (7)$$

By use of equation 7, the rough total relation matrix of IOT challenges is set as Tab. 5.

For providing the cause-effect graph, the sum of each column values and the sum of each row value of the total relationship matrix (called in turn R and D) is obtained. The higher value of (R+D) means that the relevant component has more interaction or relationships with other components and as a result, gets a lot of importance. When (D–R) has a positive value, the related component has more affection on others and vice versa. Finally, the cause-effect graph is depicted by drawing the points with the coordinates of (D+R, D–R). Before that, the sum of rows and the sum of columns are separately shown as D_i and R_j within the rough total-relation matrix T:

$$D_i = \begin{bmatrix} D_i^{L} & D_i^{U} \end{bmatrix} = \left[\sum_{j=1}^{n} t_{ij}^{L} \quad \sum_{j=1}^{n} t_{ij}^{U} \right], \quad (8)$$

$$R_i = \begin{bmatrix} R_i^{L} & R_i^{U} \end{bmatrix} = \left[\sum_{i=1}^{n} t_{ij}^{L} \quad \sum_{i=1}^{n} t_{ij}^{U} \right]. \quad (9)$$

D_i^{L} and D_i^{U} are the lower limit and upper limit values of interval rough D_i while E_i^{L} and E_i^{U} are lower limit and upper limit values of the interval rough E_i. However, to depict the cause-effect graph, it is necessary to convert these rough intervals into crisp values. D_i is converted into crisp value as such:

$$D_{i\ (Normal)}^{L} = \frac{\left(D_i^{L} - \min_i D_i^{L}\right)}{\Delta_{\min}^{\max}}, \quad (10)$$

$$D_{i\ (Normal)}^{U} = \frac{\left(D_i^{U} - \min_i D_i^{L}\right)}{\Delta_{\min}^{\max}}, \quad (11)$$

$$\Delta_{\min}^{\max} = \max_i D_i^{U} - \min_i D_i^{L}. \quad (12)$$

$D_{i\ (Normal)}^{L}$ and $D_{i\ (Normal)}^{U}$ are the normalized form of the D_i^{L} and D_i^{U} while the total normalized crisp value is specified as such:

$$\alpha_i = \frac{D_{i\ (Normal)}^{L} * (1 - D_{i\ (Normal)}^{L}) + D_{i\ (Normal)}^{U} * D_{i\ (Normal)}^{U}}{1 - D_{i\ (Normal)}^{L} + D_{i\ (Normal)}^{U}}. \quad (13)$$

Tab. 3: The rough group direct relation matrix of IOT application challenges – Part 1

CH	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	[0 0]	[4 4]	[2.04 2.36]	[3.16 3.64]	[3.16 3.64]	[2.65 3.35]	[2.16 2.64]	[3.36 3.84]	[2.64 2.96]	[3.36 3.84]	[2.52 2.92]	[2.16 2.64]	[3.16 3.64]	[3.36 3.84]	[1.75 3.08]
2	[3.16 3.64]	[0 0]	[3.36 3.84]	[3.36 3.84]	[3.36 3.84]	[3.00 3.8]	[2.746 3.64]	[2.54 3.53]	[3.16 3.64]	[3.16 3.64]	[3.16 3.64]	[3.16 3.64]	[2.86 3.64]	[4 4]	[2.86 3.64]
3	[2.46 3.534]	[2.04 2.36]	[0 0]	[2.36 2.84]	[2.16 2.96]	[2.65 3.35]	[3.04 3.36]	[2.16 2.96]	[2.36 2.84]	[2.36 2.84]	[3.16 3.64]	[2.16 2.96]	[1.46 2.53]	[1.65 2.35]	[1.65 2.35]
4	[3.36 3.84]	[2.36 2.92]	[1.16 1.64]	[0 0]	[4.00 4.00]	[3.36 3.84]	[3.16 3.64]	[3.36 3.84]	[3.36 3.84]	[3.64 3.96]	[2.16 2.64]	[2.36 2.84]	[3.64 3.96]	[4 4]	[3.16 3.64]
5	[3.36 3.84]	[2.36 2.92]	[1.04 1.36]	[4 4]	[0 0]	[3.16 3.64]	[3.04 3.36]	[3.04 3.36]	[3.64 3.96]	[3.16 3.64]	[2.04 2.36]	[2.36 2.84]	[3.64 3.96]	[3.64 3.96]	[2.65 3.35]
6	[3.4 4]	[1.74 2.64]	[3.16 3.64]	[3.64 3.96]	[4 4]	[0 0]	[1.65 2.35]	[2.64 2.96]	[2.64 2.96]	[2.64 2.96]	[2.16 2.64]	[2.64 2.96]	[2.65 3.35]	[3.16 3.64]	[3 3.8]
7	[2.16 2.64]	[3.16 3.64]	[3.36 3.84]	[3.64 3.96]	[2.65 3.35]	[3.64 3.96]	[0 0]	[2.65 3.35]	[3.16 3.64]	[2.16 2.64]	[3.04 3.36]	[3.16 3.64]	[2.16 2.96]	[2.65 3.35]	[1.36 1.84]
8	[2.692 3.252]	[1.36 2.02]	[2.36 2.84]	[2.16 2.64]	[3.00 3.00]	[1.36 2.02]	[1.94 2.47]	[0 0]	[2.16 2.96]	[2.16 2.64]	[1.64 1.96]	[1.74 2.64]	[3.16 3.64]	[3.16 3.64]	[3.36 3.84]
9	[2.16 2.64]	[3.16 3.64]	[2.64 2.96]	[3.16 3.64]	[3.16 3.64]	[1.65 2.35]	[1.744 2.64]	[2.16 2.64]	[0 0]	[2.04 2.36]	[2.36 2.84]	[2.64 2.96]	[3.04 3.36]	[3.00 3.00]	[2.65 3.35]

Tab. 3: The rough group direct relation matrix of IOT application challenges – Part 2

CH	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	[2.692 3.252]	[2.746 3.64]	[1.16 1.64]	[2.746 3.64]	[3.16 3.64]	[2.36 2.84]	[3.04 3.36]	[3.16 3.64]	[2.65 3.35]	[0 0]	[2.36 2.84]	[2.04 2.36]	[2.65 3.35]	[3 3.8]	[3.36 3.84]
11	[1.81 2.35]	[1.36 2.252]	[2.36 2.84]	[1.36 1.84]	[1.00 1.00]	[3.36 3.84]	[3.36 3.84]	[2.04 2.36]	[3 3.8]	[2.16 2.64]	[0 0]	[2.64 2.96]	[3.36 3.84]	[2.04 2.36]	[2.36 2.84]
12	[2.08 2.30]	[1.65 2.35]	[2.04 2.36]	[1.36 1.84]	[0.64 0.96]	[3.4 4.33]	[3 3.8]	[2.04 2.36]	[3.16 3.64]	[2.16 2.64]	[2.36 2.84]	[0 0]	[3.36 3.84]	[2.16 2.64]	[2.64 2.96]
13	[3.36 3.84]	[2.36 2.84]	[1.94 2.83]	[3 3.8]	[3 3.8]	[3 3.8]	[3 3.8]	[3.36 3.84]	[3.36 3.84]	[2.36 2.92]	[3.04 3.36]	[3.16 3.64]	[0 0]	[3 3.8]	[3.36 3.84]
14	[2.46 3.534]	[2.16 2.64]	[1.65 2.35]	[3.04 3.36]	[3 3.8]	[3.36 3.84]	[3.64 3.96]	[2.94 3.83]	[3 3.8]	[2.65 3.35]	[3.04 3.36]	[3.16 3.64]	[3.36 3.84]	[0 0]	[4.00 4.00]
15	[4.00 4.00]	[3.36 3.84]	[1.74 2.64]	[4.00 4.00]	[4.00 4.00]	[3.36 3.84]	[3 3.8]	[3 3.8]	[3 3.8]	[3.16 3.64]	[3.04 3.36]	[3.16 3.64]	[3.36 3.84]	[3.36 3.84]	[0 0]

Source: own

Tab. 4: Normalized rough group direct relation matrix of IOT challenges

CH	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	[0 0]	[0.07 0.07]	[0.03 0.04]	[0.06 0.06]	[0.06 0.06]	[0.05 0.06]	[0.04 0.05]	[0.06 0.07]	[0.05 0.05]	[0.06 0.07]	[0.04 0.05]	[0.04 0.05]	[0.06 0.06]	[0.06 0.07]	[0.03 0.05]
2	[0.03 0.06]	[0 0]	[0.06 0.07]	[0.06 0.07]	[0.06 0.07]	[0.05 0.07]	[0.05 0.06]	[0.04 0.06]	[0.06 0.06]	[0.06 0.06]	[0.06 0.06]	[0.06 0.06]	[0.05 0.06]	[0.07 0.07]	[0.05 0.06]
3	[0.04 0.06]	[0.03 0.04]	[0 0]	[0.04 0.05]	[0.04 0.05]	[0.05 0.06]	[0.05 0.06]	[0.04 0.05]	[0.04 0.05]	[0.04 0.05]	[0.06 0.06]	[0.04 0.05]	[0.02 0.04]	[0.03 0.04]	[0.03 0.04]
4	[0.06 0.07]	[0.04 0.05]	[0.02 0.03]	[0 0]	[0.07 0.07]	[0.06 0.07]	[0.06 0.06]	[0.06 0.07]	[0.06 0.07]	[0.06 0.07]	[0.04 0.05]	[0.04 0.05]	[0.06 0.07]	[0.07 0.07]	[0.06 0.06]
5	[0.06 0.07]	[0.04 0.05]	[0.01 0.02]	[0.07 0.07]	[0 0]	[0.06 0.06]	[0.05 0.06]	[0.05 0.06]	[0.06 0.07]	[0.06 0.06]	[0.03 0.04]	[0.04 0.05]	[0.06 0.07]	[0.06 0.07]	[0.05 0.06]
6	[0.06 0.07]	[0.03 0.05]	[0.06 0.06]	[0.06 0.07]	[0.07 0.07]	[0 0]	[0.03 0.04]	[0.05 0.05]	[0.05 0.05]	[0.05 0.05]	[0.04 0.05]	[0.05 0.05]	[0.05 0.06]	[0.06 0.06]	[0.05 0.07]
7	[0.04 0.05]	[0.06 0.06]	[0.06 0.07]	[0.06 0.07]	[0.05 0.06]	[0.06 0.07]	[0 0]	[0.05 0.06]	[0.06 0.06]	[0.04 0.05]	[0.05 0.06]	[0.06 0.06]	[0.04 0.05]	[0.05 0.06]	[0.02 0.03]
8	[0.05 0.06]	[0.02 0.03]	[0.04 0.05]	[0.04 0.05]	[0.05 0.05]	[0.02 0.03]	[0.03 0.04]	[0 0]	[0.04 0.05]	[0.04 0.05]	[0.03 0.03]	[0.03 0.05]	[0.06 0.06]	[0.06 0.06]	[0.06 0.07]
9	[0.04 0.05]	[0.06 0.06]	[0.05 0.05]	[0.06 0.06]	[0.06 0.06]	[0.03 0.04]	[0.03 0.05]	[0.04 0.05]	[0 0]	[0.03 0.04]	[0.04 0.05]	[0.05 0.05]	[0.05 0.06]	[0.05 0.05]	[0.05 0.06]
10	[0.05 0.06]	[0.05 0.06]	[0.02 0.03]	[0.05 0.06]	[0.06 0.06]	[0.04 0.05]	[0.05 0.06]	[0.06 0.06]	[0.05 0.06]	[0 0]	[0.04 0.05]	[0.03 0.04]	[0.05 0.06]	[0.05 0.07]	[0.06 0.07]
11	[0.03 0.04]	[0.02 0.04]	[0.04 0.05]	[0.02 0.03]	[0.01 0.01]	[0.06 0.07]	[0.06 0.07]	[0.03 0.04]	[0.05 0.07]	[0.04 0.05]	[0 0]	[0.05 0.05]	[0.06 0.07]	[0.03 0.04]	[0.04 0.05]
12	[0.03 0.04]	[0.03 0.04]	[0.03 0.04]	[0.02 0.03]	[0.01 0.01]	[0.06 0.07]	[0.05 0.07]	[0.03 0.04]	[0.06 0.06]	[0.04 0.05]	[0.04 0.05]	[0 0]	[0.06 0.07]	[0.04 0.05]	[0.05 0.05]
13	[0.06 0.07]	[0.04 0.05]	[0.03 0.05]	[0.05 0.07]	[0.05 0.07]	[0.05 0.07]	[0.05 0.07]	[0.06 0.07]	[0.06 0.07]	[0.04 0.05]	[0.05 0.06]	[0.06 0.06]	[0 0]	[0.05 0.07]	[0.06 0.07]
14	[0.04 0.06]	[0.04 0.05]	[0.03 0.04]	[0.05 0.06]	[0.05 0.07]	[0.06 0.07]	[0.06 0.07]	[0.05 0.07]	[0.05 0.07]	[0.05 0.06]	[0.05 0.06]	[0.06 0.06]	[0.06 0.07]	[0 0]	[0.07 0.07]
15	[0.07 0.07]	[0.06 0.07]	[0.03 0.05]	[0.07 0.07]	[0.07 0.07]	[0.06 0.07]	[0.05 0.07]	[0.05 0.07]	[0.05 0.07]	[0.06 0.06]	[0.05 0.06]	[0.06 0.06]	[0.06 0.07]	[0.06 0.07]	[0 0]

Source: own

Tab. 5: Rough total relation matrix of IOT challenges

CH	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	[0.14 0.43]	[0.20 0.46]	[0.15 0.39]	[0.21 0.50]	[0.21 0.49]	[0.19 0.50]	[0.18 0.48]	[0.20 0.50]	[0.20 0.50]	[0.20 0.47]	[0.18 0.44]	[0.17 0.45]	[0.21 0.52]	[0.22 0.51]	[0.17 0.48]
2	[0.19 0.54]	[0.13 0.43]	[0.18 0.45]	[0.22 0.55]	[0.22 0.54]	[0.21 0.56]	[0.20 0.54]	[0.20 0.54]	[0.22 0.56]	[0.20 0.51]	[0.20 0.49]	[0.20 0.51]	[0.22 0.57]	[0.24 0.56]	[0.20 0.54]
3	[0.16 0.44]	[0.14 0.38]	[0.09 0.30]	[0.16 0.43]	[0.16 0.42]	[0.16 0.45]	[0.17 0.43]	[0.15 0.43]	[0.16 0.44]	[0.15 0.40]	[0.16 0.40]	[0.15 0.40]	[0.15 0.44]	[0.15 0.43]	[0.14 0.42]
4	[0.21 0.52]	[0.18 0.46]	[0.14 0.39]	[0.17 0.45]	[0.24 0.51]	[0.22 0.53]	[0.21 0.51]	[0.22 0.52]	[0.23 0.54]	[0.21 0.49]	[0.18 0.45]	[0.19 0.47]	[0.23 0.55]	[0.24 0.54]	[0.21 0.51]
5	[0.21 0.50]	[0.17 0.44]	[0.13 0.37]	[0.23 0.51]	[0.16 0.43]	[0.21 0.51]	[0.20 0.49]	[0.20 0.49]	[0.22 0.52]	[0.20 0.47]	[0.17 0.43]	[0.18 0.45]	[0.23 0.53]	[0.23 0.52]	[0.20 0.49]
6	[0.20 0.50]	[0.16 0.43]	[0.16 0.40]	[0.21 0.50]	[0.22 0.49]	[0.15 0.44]	[0.17 0.46]	[0.19 0.48]	[0.20 0.50]	[0.18 0.45]	[0.17 0.43]	[0.18 0.45]	[0.20 0.51]	[0.21 0.50]	[0.19 0.49]
7	[0.18 0.47]	[0.18 0.44]	[0.17 0.41]	[0.21 0.50]	[0.19 0.48]	[0.21 0.51]	[0.14 0.42]	[0.19 0.48]	[0.20 0.51]	[0.17 0.44]	[0.18 0.44]	[0.19 0.46]	[0.19 0.50]	[0.20 0.50]	[0.16 0.46]
8	[0.16 0.43]	[0.13 0.37]	[0.13 0.35]	[0.16 0.42]	[0.18 0.42]	[0.15 0.42]	[0.15 0.41]	[0.12 0.37]	[0.16 0.44]	[0.15 0.39]	[0.14 0.37]	[0.14 0.39]	[0.18 0.46]	[0.18 0.45]	[0.18 0.44]
9	[0.17 0.44]	[0.17 0.42]	[0.15 0.37]	[0.19 0.46]	[0.19 0.45]	[0.16 0.45]	[0.16 0.44]	[0.17 0.44]	[0.14 0.41]	[0.16 0.41]	[0.16 0.40]	[0.17 0.42]	[0.19 0.48]	[0.19 0.46]	[0.18 0.45]
10	[0.18 0.48]	[0.17 0.44]	[0.13 0.37]	[0.19 0.49]	[0.20 0.48]	[0.18 0.49]	[0.19 0.48]	[0.19 0.48]	[0.19 0.50]	[0.13 0.39]	[0.17 0.43]	[0.16 0.43]	[0.19 0.51]	[0.20 0.50]	[0.19 0.49]
11	[0.15 0.40]	[0.13 0.36]	[0.13 0.34]	[0.15 0.40]	[0.14 0.37]	[0.18 0.44]	[0.17 0.42]	[0.15 0.40]	[0.18 0.44]	[0.15 0.38]	[0.11 0.32]	[0.16 0.39]	[0.18 0.45]	[0.16 0.41]	[0.16 0.41]
12	[0.15 0.40]	[0.13 0.36]	[0.13 0.33]	[0.15 0.40]	[0.13 0.37]	[0.18 0.44]	[0.17 0.42]	[0.15 0.40]	[0.18 0.44]	[0.15 0.38]	[0.15 0.37]	[0.11 0.33]	[0.18 0.45]	[0.16 0.42]	[0.16 0.41]
13	[0.21 0.53]	[0.17 0.46]	[0.15 0.42]	[0.21 0.53]	[0.21 0.52]	[0.21 0.54]	[0.20 0.52]	[0.21 0.52]	[0.22 0.55]	[0.18 0.48]	[0.19 0.47]	[0.20 0.49]	[0.16 0.49]	[0.22 0.54]	[0.21 0.52]
14	[0.19 0.52]	[0.17 0.46]	[0.15 0.41]	[0.21 0.52]	[0.21 0.51]	[0.22 0.54]	[0.21 0.52]	[0.20 0.52]	[0.21 0.54]	[0.19 0.48]	[0.19 0.46]	[0.20 0.49]	[0.22 0.55]	[0.16 0.47]	[0.22 0.52]
15	[0.23 0.55]	[0.20 0.50]	[0.16 0.43]	[0.25 0.55]	[0.24 0.54]	[0.23 0.56]	[0.22 0.54]	[0.22 0.54]	[0.23 0.57]	[0.21 0.51]	[0.21 0.49]	[0.21 0.51]	[0.24 0.58]	[0.24 0.56]	[0.16 0.48]

Source: own

At last, final crisp values D_i are determined as follows:

$$D_i = \min_i D_i^L + \alpha_i \Delta_{\min}^{\max} \quad (14)$$

The same trend should be followed to determine the crisp value of R_i. As such, D_i and R_i rough values related to IOT challenges mutual relationships and their crisp values can be seen in Tab. 6.

Based on the crisp values of (D+R) and (D-R), the cause-effect graph is depicted (Fig. 1). Considering the values of (D-R), it can be said that "Lack of strategy and scenario planning in IOT" (CH2), "Storage issues" (CH3), "Lack of security" (CH4), "Lack of privacy" (CH5), "Responsibility sharing" (CH10) and "Dynamic environment" (CH15) constitute the cause group. All of these components can direct the entire system of challenges. It means that by managing them in the correct way, other challenges would be managed too. While the other challenges determine the effect group and take affections from the entire system of these challenges.

From other point of view, it should be said that "Legal framework for IOT governance"

Tab. 6: D_i and R_i rough and crisp values of IOT challenges

	D		R		D+R	D-R
	Rough Value	Crisp Value	Rough Value	Crisp Value		
1	[2.89 7.19]	4.99	[2.79 7.19]	5.03	10.028780	-0.033400
2	[3.11 7.95]	5.70	[2.49 6.48]	4.30	10.012860	1.400577
3	[2.31 6.29]	3.96	[2.20 5.78]	3.62	7.588406	0.331970
4	[3.16 7.51]	5.42	[3.00 7.27]	5.23	10.656390	0.185173
5	[3.02 7.22]	5.12	[2.96 7.09]	5.07	10.193390	0.046684
6	[2.87 7.10]	4.91	[2.93 7.43]	5.30	10.218740	-0.389230
7	[2.82 7.07]	4.86	[2.81 7.16]	5.01	9.881266	-0.150710
8	[2.40 6.18]	3.94	[2.82 7.15]	5.02	8.970417	-1.072640
9	[2.62 6.54]	4.35	[3.01 7.53]	5.43	9.790052	-1.083280
10	[2.74 7.03]	4.77	[2.72 6.76]	4.66	9.444452	0.113948
11	[2.35 6.00]	3.80	[2.63 6.45]	4.38	8.189256	-0.581610
12	[2.35 5.99]	3.78	[2.68 6.71]	4.60	8.389587	-0.814390
13	[3.01 7.66]	5.42	[3.06 7.64]	5.55	10.976480	-0.133900
14	[3.03 7.57]	5.37	[3.08 7.44]	5.42	10.791780	-0.049600
15	[3.32 7.98]	5.88	[2.81 7.17]	5.02	10.911120	0.858445

Source: own

(CH13) and "Dynamic environment" (CH15) have the highest level of interactions with other challenges.

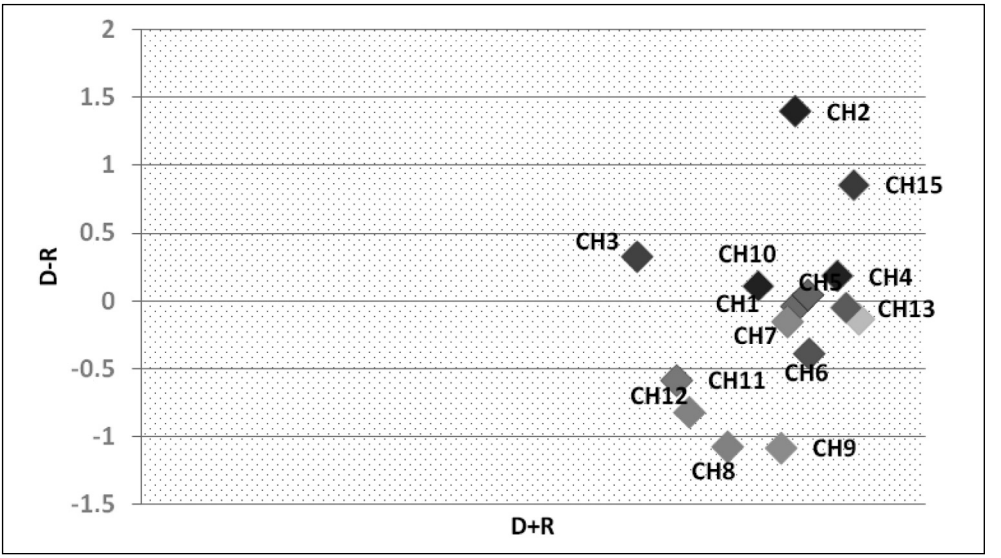
3. Discussion and Managerial Implications

It was determined that "Lack of strategy and scenario planning in IOT" (CH2) is in the cause group. There is no doubt that IOT is fast becoming entrenched both in consumer and enterprise IT systems. IOT is being discussed across all parts of supply chain. IOT can empower IT system. Even when products can be easily equipped with sensors, companies count on business models driven by IOT. So, the Internet of Things is an undeniable part of an overall digital strategy, established to enable efficiency and effectiveness. Digital strategy role is to pave the way for change within an organization.

Managers can take an incremental trend for compilation IOT scenarios taking the chance to go through the learning curve step by step. Setting some scenarios that allow operational efficiency for a specific process constitutes a good beginning to show what is possible. In this way, staff and even consumers get an understanding of the power of the Internet of Things, and then become willing to create more detailed scenarios and an integrated IOT strategy, which can be run on a large scale.

Since companies are intended to capture data and use huge data as soon as they understand what to do with the data and how to process it, "Storage issues" (CH3) is among the challenges that constitute the cause group. IOT causes more huge data to be created and most of this data can never be created again. Especially when handling sensor data, as most backup applications don't handle billions of data completely. The challenges that such data bring to storage also encompass data protection. So, the data generated from the Internet of Things has

Fig. 1: Cause-effect graph of IOT challenges



Source: own

a big impact on data protection in comparison to conventional data.

Managers should consider that storing data in isolated systems can't solve their volume and performance problem. They should think of scale-out, virtualization and cloud computing considering integrated data protection with the archive process. As data being preserved on the disk cache, copies can be made to multiple devices. This provides the chance to quickly transform data from merely interesting to object-oriented and useful for making analysis, and also foremost protection and retrieve.

"Lack of security" (CH4) and "Lack of privacy" (CH5), are the other challenges that shape the cause group. Companies applying IOT should establish reasonable security and privacy preserving approaches. Now, digital security and privacy is considered to be different from online security or privacy. Digital safety and privacy are considered as principles that protect people from menace in facing with increasingly semi-autonomous systems that are combined by various companies (Vinton et al., 2016). Conducting a privacy or security risk assessment, minimizing the data collection and retain and testing the security measures before launching the products can be helpful in minimization of security and privacy challenges. Employees should be trained about good security and privacy, and ensure that such issues are addressed.

It should be noted that privacy and safety preservation in IOT application is a shared responsibility. This put "responsibility sharing" (CH10) in cause group. Multi-stakeholder governance can be considered to address safety challenges (Vinton et al., 2016).

"Dynamic environment" (CH15) is the last challenge that constitutes the cause group in this study. Application of IOT in such a turbulence environment is a complex process. The data that should be analyzed is various and complicated and a series of highly correlated processes are undertaken to shape a product or service. Responsibilities of these processes should be shared among all stakeholders and legal framework should be established to construct a problem-solving network in such a messed up and dynamic environment (Chen et al., 2016).

Conclusions

To identify the challenges of IOT application in supply chain management, an approach based

on rough theory and the group DEMATEL method was developed in current paper. This study values are set as such that the applied rough group DEMATEL simultaneously addresses the internal strength and external affections of IOT application in supply chain management. This is important since makes the investigation of challenges possible and determines priorities for receiving attention more accurately. The rough group DEMATEL does not need much prior information for decision making in comparison to fuzzy theory. Besides, this method deals with the vague, subjective information and the uncertainty in judgments. Managers can perceive the challenges waiting for them on the path to apply IOT in supply chain management. In this way, they become equipped to face with key emerging challenges and related consequences that can affect supply chain performance.

As became clear, "Lack of strategy and scenario planning in IOT" (CH2), "Storage issues" (CH3), "Lack of security" (CH4), "Lack of privacy" (CH5), "Responsibility sharing" (CH10) and "Dynamic environment" (CH15) are the challenges with high affection on others. So, these challenges should receive more attention. Managing them causes other challenges to be managed correctly too.

This study can make a path for a variety set of future studies. It is recommended to determine a study deign to see which supply chains are successful in reducing the risk of facing these challenges. The efficiency of performance of supply chains can be compared with each other based on these challenges and by the use of Data Envelopment Analysis (DEA). Besides, it can be seen how managing these challenges can result to sustainable reputation of supply chains in the eyes of different groups of society members.

References

Addo-Tenkorang, R., & Helo, P. T. (2016). Big data applications in operations/supply-chain management: A literature review. *Computers & Industrial Engineering*, *101*, 528-543. https://dx.doi.org/10.1016/j.cie.2016.09.023.

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, *56*, 122-140, https://dx.doi.org/10.1016/j.adhoc.2016.12.004.

Banafa, A. (2016). IOT Standardization and Implementation Challenges. *IEEE*. Retrieved April 2017 from http://IOT.ieee.org/newsletter/july-2016/IOT-standardization-and-implementation-challenges.html.

Chen, Y., Lee, G. M., Shu, L., & Crespi, N. (2016). Industrial internet of things-based collaborative sensing intelligence: framework and research challenges. *Sensors*, *16*(2), 215, https://dx.doi.org/10.3390/s16020215.

Debnath, A., Roy, J., Kar, S., Zavadskas, E. K., & Antucheviciene, J. (2017). A hybrid MCDM approach for strategic project portfolio selection of agro by-products. *Sustainability*, *9*(8), 1302. https://dx.doi.org/10.3390/su9081302.

Dutton, W. H. (2014). Putting things to work: social and policy challenges for the Internet of things. *Info*, *16*(3), 1-21. https://dx.doi.org/10.1108/info-09-2013-0047.

Ebrahimnejad, S., Naeini, M. A., Ebrahimnejad, & Mousavi, S. (2017). Selection of IT outsourcing services' activities considering services cost and risks by designing an interval-valued hesitant fuzzy-decision approach. *Journal of Intelligent & Fuzzy Systems, 32*(6), 4081-4093. https://dx.doi.org/10.3233/JIFS-152520.

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2017). Towards fog-driven IOT eHealth: Promises and challenges of IOT in medicine and healthcare. *Future Generation Computer Systems*, *78*(2), 659-676. https://dx.doi.org/10.1016/j.future.2017.04.036.

Fernandez-Gago, G., Moyano, F., & Lopez, J. (2017). Modelling Trust Dynamics in the Internet of Things. *Information Sciences*, *396*, 72-82. https://dx.doi.org/10.1016/j.ins.2017.02.039.

Foroozesh, N., Tavakkoli-Moghaddam, R., & Mousavi, S. M. (2017). Resilient Supplier Selection in a Supply Chain by a New Interval-Valued Fuzzy Group Decision Model Based on Possibilistic Statistical Concepts. *Journal of Industrial and Systems Engineering, 10*(2), 113-133.

Gandhi, S., Mangla, S. K., Kumar, P., & Kumar, D. (2015). Evaluating factors in implementation of successful green supply chain management using DEMATEL: A case study. *International Strategic Management Review*, *3*(1-2), 96-109. https://dx.doi.org/10.1016/j.ism.2015.05.001.

Gill, A. Q., Phennel, N., Lane, D., & Phung, V. L. (2016). IOT-enabled Emergency

Information Supply Chain Architecture for Elderly People: The Australian Context. *Information Systems*, *58*, 75-86, https://dx.doi.org/10.1016/j.is.2016.02.004.

Hsu, C. W., & Yeh, C. C. (2016). Understanding the factors affecting the adoption of the Internet of Things. *Technology Analysis & Strategic Management*, *29*(9), 1089-1102, https://dx.doi.org/10.1080/09537325.2016.1269160.

IERC. (2015). *Internet of Things - IOT Governance, Privacy and Security Issues.* European Research Cluster on The Internet Of Things.

Jian, L., Liu, S., & Lin, Y. (2011). *Hybrid Rough Sets and Applications in Uncertain Decision-Making*. Auerbach Publications.

Kees, A., Oberländer, A., Röglinger, M., & Rosemann, M. (2015). Understanding the Internet of Things: A Conceptualisation of Business-To-Thing (B2T) Interactions. In *The Proceedings of Twenty-Third European Conference on Information Systems (ECIS)* (pp. 1-16). Münster, Germany.

Kim, S., & Kim, S. (2016). A multi-criteria approach toward discovering killer IOT application in Korea. *Technological Forecasting and Social Change*, *102*, 143-155. https://dx.doi.org/10.1016/j.techfore.2015.05.007.

Krotov, V. (2017). The Internet of Things and new business opportunities. *Business Horizons*, *60*(6), 831-841. https://doi.org/10.1016/j.bushor.2017.07.009.

Lee, H. (2017). Framework and development of fault detection classification using IOT device and cloud environment. *Journal of Manufacturing Systems*, *43*(2), 257-270. https://dx.doi.org/10.1016/j.jmsy.2017.02.007.

Liou, J. J. H., Tamosaitiene, J., Zavadskas, E. K., Tzeng, G. H. (2016). New hybrid COPRAS-G MADM model for improving and selecting suppliers in green supply chain management. *International Journal of Production Research*, *54*(1), 114-134. https://dx.doi.org/10.1080/00207543.2015.1010747.

Lu, M. T., Lin, S. W., & Tzeng, G. H. (2013). Improving RFID adoption in Taiwan's healthcare industry based on a DEMATEL technique with a hybrid MCDM model. *Decision Support Systems*, *56*, 259-269. https://dx.doi.org/10.1016/j.dss.2013.06.006.

Mardani, A., Nilashi, M., Antucheviciene, J., Tavana, M., Bausys, R., & Ibrahim, O. (2017). Recent fuzzy generalisations of rough sets theory: a systematic review and methodological critique of the literature. *Complexity*, *2007*. https://dx.doi.org/10.1155/2017/1608147.

Mital, M., Choudhary, P., Chang, V., Papa, A., & Pani, A. K. (2017). Adoption of Internet of Things in India: A test of competing models using a structured equation modeling approach. *Technological Forecasting & Social Change*, *In Press*. https://dx.doi.org/10.1016/j.techfore.2017.03.001.

Meola, M. (2016). *How IOT logistics will revolutionize supply chain management.* Retrieved 10th August, 2017, from http://www.businessinsider.com/internet-of-things-logistics-supply-chain-management-2016-10.

Park, K. C., & Shin, D. H. (2017). Security assessment framework for IOT service. *Telecommunication Systems*, *64*(1), 193-209. https://dx.doi.org/10.1007/s11235-016-0228-5.

Pourahmad, A., Hosseini, A., Banaitis, A., Nasiri, H., Banaitienė, N., & Tzeng, G. H. (2015). Combination of fuzzy–AHP and DEMATEL–ANP with GIS in a new hybrid MCDM model used for the selection of the best space for leisure in a blighted urban site. *Technological and Economic Development of Economy, 21*(5), 773-796. https://dx.doi.org/10.3846/20294913.2015.1056279.

Rajesh, R., & Ravi, R. (2015). Modeling enablers of supply chain risk mitigation in electronic supply chains: A Grey–DEMATEL approach. *Computers & Industrial Engineering*, *87*, 126-139. https://dx.doi.org/10.1016/j.cie.2015.04.028.

Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2017). A Roadmap for Security Challenges in Internet of Things. *Digital Communications and Networks*. In press. https://doi.org/10.1016/j.dcan.2017.04.003.

Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? *Business Horizons*, *60*(5), 667-676. https://dx.doi.org/10.1016/j.bushor.2017.05.010.

Shankar, U. (2017). *How the Internet of Things Impacts Supply Chains. In bound Logistics, white paper*. Retrieved 10th April, 2017, from http://www.inboundlogistics.com/cms/article/how-the-internet-of-things-impacts-supply-chains/

Song, W., Ming, X., & Liu, H. C. (2017). Identifying critical risk factors of sustainable supply chain management: A rough strength-relation analysis method. *Journal of Cleaner Production, 143*, 100-115. https://dx.doi.org/10.1016/j.jclepro.2016.12.145.

Supeekit, T., Somboonwiwat, T., & Kritchanchai, D. (2016). DEMATEL-modified

ANP to evaluate internal hospital supply chain performance. *Computers & Industrial Engineering*, *102*, 318-330. https://dx.doi.org/10.1016/j.cie.2016.07.019.

Teixeira, F. A., Pereira, F. M. Q., Wong, H. C., Nogueira, J. M. S., & Oliveira, L. B. (2017). SIOT: Securing Internet of Things through distributed systems analysis. *Future Generation Computer Systems*. In Press. https://doi.org/10.1016/j.future.2017.08.010.

Verdouw, C. N., Beulens, A. J. M., & van der Vorst, J. G. A. J. (2013). Virtualisation of floricultural supply chains: A review from an Internet of Things perspective. C*omputers and Electronics in Agriculture*, *99*, 160-175. https://dx.doi.org/10.1016/j.compag.2013.09.006.

Verdouw, C. N., Wolfert, J., Beulens, A. J. M., & Rialland, A. (2015). Virtualization of food supply chains with the internet of things. *Journal of Food Engineering*, *176*, 128-136, https://dx.doi.org/10.1016/j.jfoodeng.2015.11.009.

Vinton, G. C., Ryan, P. S., Senges, M., & Whitt, R. S. (2016). IOT Safety and Security as Shared Responsibility. *Journal of Business Informatics*, *35*(1), 7-19.

Weber, R. H. (2013). Internet of things – Governance quo vadis? *Computer Law & Security Review*, *29*(4), 341-347. https://dx.doi.org/10.1016/j.clsr.2013.05.010.

Woodside, A. G., Megehee, C. M., & Sood, S. (2012). Conversations with (in) the collective unconscious by consumers, brands, and relevant others. *Journal of Business Research*, *65*(5), 594-602. https://dx.doi.org/10.1016/j.jbusres.2011.02.016.

Yupeng, L., Yifei, C., & Tzeng, G. H. (2017). Identification of key factors in consumers' adoption behavior of intelligent medical terminals based on a hybrid modified MADM model for product improvement. *International Journal of Medical Informatics*, *105*, 68-82, https://dx.doi.org/10.1016/j.ijmedinf.2017.05.017.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & Alvarenga, S. T. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Application*s, *84*, 25-37. https://dx.doi.org/10.1016/j.jnca.2017.02.009.

Zhai, L. Y., Khoo, L. P., & Zhong, Z. W. (2009). Design concept evaluation in product development using rough sets and gray relation analysis. *Expert Systems with Applications*, *36*(3), 7072-7079. https://dx.doi.org/10.1016/j.eswa.2008.08.068.

Visiting Lecturer, Mahsa Pishdar, PhD.
Allameh Tabataba'i University
Faculty of Accounting and Management
Department of Industrial Management
Iran
mahsa.pishdar@yahoo.com

Visiting Lecturer, Fatemeh Ghasemzadeh, PhD.
Allameh Tabataba'i University
Faculty of Accounting and Management
Department of Industrial Management
Iran
ghasemzadeh.fa@gmail.com

Prof. Jurgita Antucheviciene, Ph.D.
Vilnius Gediminas Technical University
Faculty of Civil Engineering
Department of Construction Management and Real Estate
Lithuania
jurgita.antucheviciene@vgtu.lt

Assoc. Prof. Jonas Saparauskas, Ph.D.
Vilnius Gediminas Technical University
Faculty of Civil Engineering
Department of Construction Management and Real Estate
Lithuania
jonas.saparauskas@vgtu.lt

Abstract

INTERNET OF THINGS AND ITS CHALLENGES IN SUPPLY CHAIN MANAGEMENT: A ROUGH STRENGTH-RELATION ANALYSIS METHOD

Mahsa Pishdar, Fatemeh Ghasemzadeh, Jurgita Antucheviciene, Jonas Saparauskas

Internet of Things application (IOT) in supply chain management is becoming imperative and can shape a strategic competitive advantage. Albeit, different challenges appear through this application, most of the previous studies consider less about these challenges and focus on the advantages of IOT. To overcome this defect, different challenges that a supply chain may face as whole are determined based on systematic literature review and expert opinions. Then, a rough group decision-making and trial evaluation laboratory (DEMATEL) is applied. Advantages of the proposed model are that both internal strength and external influence of challenges and also vagueness and ambiguity of experts' opinions are simultaneously noticed to completely show the importance of these challenges. The results show that challenges such as lack of strategy and scenario planning in IOT, storage issues, lack of security and lack of privacy are of great importance. So, these challenges should have a higher priority in attracting attention and resources. These results help managers to be equipped to face with main challenges in their path toward IOT in their supply chains. Accordingly some practical suggestions for managers are discussed in this paper, such as starting the journey toward IOT step by step, planning for a data storage system which is appropriate for big data, setting up a security policy to prevent out-coming problems caused by lack of security and privacy inherited by IOT, conducting a privacy or security risk assessment, minimizing the data collection and retain and testing the security measures before launching the products, and establishment of a legal framework to construct a problem-solving network in such a messed up and dynamic environment for processing such complicated huge data.

Key Words: *Group decision making, group DEMATEL, internet of things (IOT), risk management, rough set theory, supply chain management.*

JEL Classification: *O33, D81, M15.*

DOI: *10.15240/tul/001/2018-2-014*