Ferdowsi University of Mashhad
Systems Thinking in Practice
3rd International Conference on
سومین کنفرانس بین المللی
تفکر سیستمی در عمل

Prioritizing of The Internet of Manufacturing Things (IoMT) Challenges in Automotive Industry by using Interpretive Structural Modeling (ISM)

Sahar Valipour Parkouhi[1], Abdolhamid Safaei Ghadikolaei[2], Hamidreza Fallah Lajimi[3]

[1]PhD candidate, University of Mazandaran
[2]Professor, University of Mazandaran
[3]Assistant Profosssor, University of Mazandaran
* Abdolhamid Safaei Ghadikolaei

ABSTRACT

Smart manufacturing can be referred as an important consequence of Fourth Industrial Revolution. With the advent of this revolution, manufacturing companies must use numerous new technologies to become smart. According to these new technologies, companies face multifaceted challenges. The Internet of Things (IoT) technology is one of the achievements of Industry 4.0, which plays an important role in the implementation of smart manufacturing. IoT using in smart manufacturing is called Internet of Manufacturing Things (IoMT Like other technologies, IoMT has its own challenges. Therefore, manufacturing organizations must be able to identify these challenges and concentrate on them based on their priority. In this study, by reviewing the literature, the challenges of using the Internet of Things in smart manufacturing were identified. Then Interpretive Structural Modeling (ISM) technique was used to prioritize challenges in the automotive industry. Based on the research findings, the challenges were classified into three levels. This leveling provides a suitable model for automotive industry managers to be able to prioritize their strategies and actions accordingly..

Keywords: Smart manufacturing, Internet of things, Internet of Manufacturing Things (IoMT), Challenges, Interpretive Structural Modeling (ISM).

1. Introduction

In recent years, in the field of wireless communications and networking, a new paradigm called the Internet of Things (IoT) has attracted the attention of many researchers and industrialists. The Internet of Things can be defined as a network of physical objects that are digitally connected so that they could sense, monitor, and influence each other (Xu et al. 2022). A supply chain is also a network that requires monitoring and control of relationships between components. Therefore, the use of IoMT in different parts of the supply chain can facilitate communication and cooperation between partners and processes within it. By using the Internet of Things in manufacturing (as part of supply chain processes), smart manufacturing is formed. According to the definition presented by Smart Manufacturing Leadership Coalition (SMLC), smart manufacturing is "*the right data in the right form, the right people with the right knowledge, the right technology, and the right operations, whenever and wherever the production needed throughout the manufacturing enterprise*" (Edgar and Pistikopoulos 2018). Another definition was provided by National Institute of Standard and Technology, (NIST), based on which smart manufacturing is "*fully integrated, collaborative manufacturing systems that respond in real time to meet changing demands and conditions in the factory, in the supply network, and in customer needs*".

As with previous manufacturing parameters, smart manufacturing has also developed in the automotive industry. The automotive industry is regarded as a key industry in terms of its extensive relationship with a chain of industries before and after it and has a high potential for economic development. As stated in the philosophy of production paradigms, concepts such as mass production, lean production and world-class manufacturing, which have revolutionized various industries, were first introduced and implemented for in the automotive industry (mass production at Ford Motor Company, Lean production and World Class manufacturing in Toyota company). (Ebrahimi, Baboli, and Rother 2019). Consequently, the present study seeks to examine the challenges of the Internet of Things in smart manufacturing as a new production paradigm in the automotive industry.

In addition to the dramatic change in the automotive industry, the Internet of Things has affected the performance of automakers and the software they use, thus trying to maximize values (Krasniqi and Hajrizi 2016). Smartening the automotive industry will bring benefits such as lower costs, energy savings, environmental protection, and efficient after-sales service (Liu et al. 2012). To achieve these goals, there are serious challenges in smartening and implementing IoMT. In the last decade, these challenges have been introduced in conducted research in the field of smart manufacturing and the Internet of Things. (Afzal et al. 2019; Chen et al. 2014; Cooper and James 2009; Farahani et al. 2018; Furnell et al. 2009; Kumar and Mallick 2018; Lee and Lee 2015; Lim, Kim, and Maglio 2018; Makhdoom et al. 2019; Reyna et al. 2018), However, but it is not possible to consider and address all challenges simultaneously. Therefore, it must be determined at what level each challenge is and which challenges are prioritized. Using ISM technique to level the challenges and consequently their management in IoMT deployment is also considered as an contribution of the innovation in the present study.

This paper is organized as follows. In section 2, the IoMT implementation challenges were extracted by reviewing the IoMT literature and its application in smart manufacturing. Section 3 describes the steps of research and ISM technique. Section 4 includes the leveling of the challenges introduced in this research. Finally, section 5 presents the results of the research.

2. Literature and Research Background

2-1. Internet of Things (IoT) and Internet of manufacturing Things (IoMT)

The Internet Plus initiative has been developed by Chinese Premier Li Keqiang as a way to accelerate China's slowing economy. This initiative aims to link the Internet and related information technology fields to current industries to increase productivity and economic growth. Cloud computing, mobile Internet, big data utilization, the Internet of Things, etc can be considered as the pillars of Internet Plus (Hristov 2017).

The Internet of Things was first introduced by Kevin Ashton in 1999 through the Auto-ID Center at MIT. For Ashton, "Internet of Things" means all objects and people equipped with computers, sensors, and the Internet that can be managed. He also introduced Radio-frequency identification (RFID) as a prerequisite for it (Dhumale1, Thombare, and Bangare 2017). The Internet of Things has features such as connectivity to remote data collection, analysis, and management capabilities that minimize human intervention in the production, transmission, and use of data (Rose et al. 2015)

There are two different aspects to the Internet of Things (See Figure (1)): Information Technology (IT) and Operational Technology (OT) (Khan, Khan, and Haleem 2020) .. IT is the “objects” such as servers, databases, and applications. Networks run these objects while IT controls them. IT makes sure that the connections between data in a company are safe and reliable. OT is mainly concerned with industrial interactions. This aspect consists of sensors, systems connected to machines, and other types of equipment that control the performance of physical systems. Before IoT, two concepts of IT and OT were two different poles that worked separately and did not need to interact with each other. However, IoT is here to combine these two concepts as it is based on a world of inter-related objects (Khan et al. 2020).

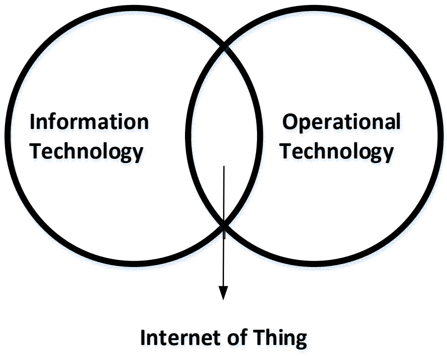

Figure 1. Venn Diagram of IoT (Khan et al. 2020)

According to research conducted in this area, several researchers have proposed some definitions for IoT (Table 1), although there is an overlap in these definitions.

Table 1. Definition of IoT

References	Definitions
(Satyavolu et al. 2014)	The Internet of Things includes objects or 'things' that have sensors embedded in them to enable them to communicate its state with other objects and automated systems in the environment.
(Dorsemaine et al. 2016).	IoT *"connects a group of interconnected infrastructures and objects and allows their management to extract and analyze data. In IoT, connected objects are sensors that create a specific function and communicate with other equipment*".
(Rose et al. 2015)	The term IoT refers to the extension of network connectivity and the capability to compute objects, devices, and sensors that are not normally considered as computers. These smart objects require minimal human intervention in the production, exchange and consumption of data. They often include the feature of connectivity to remote data collection, analysis and management capabilities.

The objects mentioned in the above definitions represent a node in a virtual network that continuously transmits a large volume of data about itself and other network components (Satyavolu et al., 2014). Things that are deployed in IoT are (i) RFID tags, for unique identification, (ii) sensors, for detecting physical changes in the environment, and (iii) actuators, for transmitting information to the environment (Lanotte and Merro 2018).

In IoT, objects are generally objects of the physical things or virtual things that can be identified and integrated into communication network Physical objects exist in the physical world and are capable to be sensed and / or actuated upon and / or connected. sensors of surrounding environments, industrial robots, goods, and electrical equipment are examples of physical objects. Virtual objects exist in the virtual world and have the capability to be stored, processed and accessed. Examples of virtual objects are multimedia contents, application software, and service representations of physical things (Lee1 et al. 2013).

The end point of communication in IoT can be humans or objects (devices / machines). As a consequence, two categories of communication are considered for IoT (Lee1 et al. 2013). Human-to-Object (Thing) Communication: Humans communicate with a device to obtain specific information, which includes remote access to objects by humans. Object-to-Object (Thing-to-Thing) Communication: An Object delivers information to another object that may or may not be human.

Before industrialization, most of the work had to be done by manpower. After the first industrial revolution, machines and human resources started a corroboration by which the manufacturing time was reduced, the quality of the products was increased, and the general productivity was ameliorated. Even now, in the era of the Fourth Industrial Revolution, Technologies like IoT are used to improve productivity, reliability, and accessibility of financial resources to open new doors to how products are made and introduced to the market. Internet of Manufacturing Technology (IoMT) is the application of IoT in Manufacturing. IoT systems are introduced in the previous section. Before defining IoMT, it is better to define Manufacturing Things. Manufacturing Things are all the essential instruments and physical equipment a factory needs to turn raw material into the finished product. Workforce, machines, work-in-progress items, and many other company objects are considered manufacturing things (Zhang et al. 2014). IoMT is an optimized system for managing driving manufacturing data that optimally control manufacturing processes from placing the orders to manufacturing the finished product and selling it (Zhang et al. 2014). In another sense, IoMT is all the manufacturing steps, processes, and generally the whole manufacturing cycle in a factory. IoMT is an open network system that combines advanced manufacturing, IoT, information, and modern management (Li et al. 2018). IoM has two parts: software and hardware. Hardware is all the Auto-ID systems that hold manufacturing data, while software is several application services responsible for backing up the decision-making process (Zhang et al. 2014).

The application of the Internet of Things in smart manufacturing

The application of IoT in various fields is increasing rapidly. The Internet of Things can be used in a variety of areas, including smart manufacturing, smart grid, smart healthcare, smart home, and smart city.

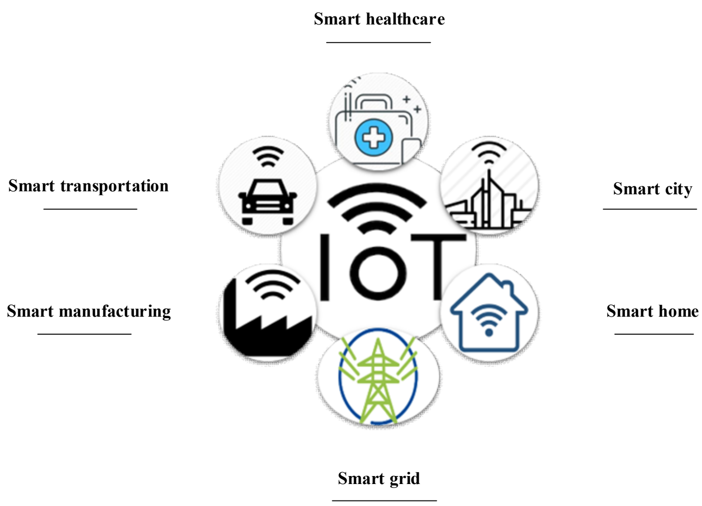

Figure 2. IoT Application

As can be seen in Figure (2), one of the application of the Internet of Things is in smart manufacturing. The goal of smart manufacturing is to improve productivity, efficiency, reliability and better control of final products (Kouicem, Bouabdallah, and Lakhlef 2018). Smart manufacturing includes new technologies such as machine-to-machine (M2M) communication, wireless sensor networks (WSNs), automation technologies, as well as big data and the Internet of Things.

The IoT approach is an ideal solution for automating and controlling the manufacturing process and plays an important role in creating a communication infrastructure for information acquisition and its sharing. Real-time data of actuators is not limited and resilient to changes, but RFID and WSN are effective tools in supporting the distribution and decentralization of production resources. The IoT architecture is dynamic which facilitates the integration of information by combining the host company and other virtual companies to conduct projects throughout the company. Dynamic relationships are created for specific projects. After the completion of the project, this combination can be changed and the company is ready to do another project. To conduct manufacturing projects, some human-to-human, human-to-object, and object-to-object interactions take place. With the development of the Internet of Things, all of these interactions can be integrated. In this way, partners can focus on multiple decisions that require integrated and compact information and high computing power, rather than worrying about interactions. Manufacturing companies use multiple computer resources such as servers and databases as well as decision units. This leads to the waste of investment, failure in utilization of production resources, low productivity and improper information exchange among servers. Cloud computing provides a vital solution to these problems. All data is stored on public or private cloud servers, and complex decisions can be supported using cloud computing (Zhuming Bi, Li Da Xu, and Chengen Wang 2014). According to the stated cases above, IoT affects all parts of the production chain (communications, information, decision-making, etc.). Therefore, examining the challenges of implementing IoT in manufacturing companies can in be identifying critical points and taking necessary actions measures.

2-2. Challenges of using IoMT in manufacturing

The development and application of IoMT affects various aspects of human life (such as security, healthcare, productivity, energy, environmental sustainability, etc.). A review of the literature revealed that IoMT challenges were introduced in various fields such as healthcare and treatment (Farahani et al. 2018) and blockchain (Kumar and Mallick 2018; Makhdoom et al. 2019). Many studies have examined the conceptual study of this field (Afzal et al. 2019; Chen et al. 2014; Cooper and James 2009; Farahani et al. 2018; Furnell et al. 2009; Khan and Salah 2018; Kumar and Mallick 2018; Makhdoom et al. 2019; Reyna et al. 2018). Some studies have specifically identified security challenges (Khan and Salah 2018; Kumar and Mallick 2018) and data management challenges (Cooper and James 2009). The gap seen in the literature is the study of the challenges of the Internet of Things in the manufacturing industry. IoMT implementation and deployment in the manufacturing industry requires infrastructure that is certainly associated with organizational, hardware, and software issues and challenges. By reviewing the literature on the application of IoMT in smart manufacturing, the challenges of Table (2) were identified.

Table 2. Challenges of using . IoMT

Challenges		Definition	References
Data management and integrity	C_1	Applying the IoMT approach creates a large amount of homogeneous and heterogeneous data; data analysis in different time periods can produce practical results for the organization. Most data centers do not have the capability to process, integrate and store this data on individual or organizational dimensions.	(Cooper and James 2009; Farahani et al. 2018; Kamali et al. 2018; Lee and Lee 2015; Lim et al. 2018; Nasrollahi and Ramezani 2020)
Sensitive data access control	C_2	With the deployment of the IoMT approach and due to wide variety of data types, the level of user access to important and sensitive data is critical for the organization and the lack of a coherent strategy for how users access, disrupts the security of the information system.	(Furnell et al. 2009)
Storage capacity and scalability	C_3	In IoMT, data and equipment integration is critical; therefore, all processes and devices need to be considered at maximum capacity so that in case of their development, there will be no disruption to their speed and utilization for stakeholders. This is possible by using tools such as smartphones.	(Farahani et al. 2018; Reyna et al. 2018)
User privacy	C_4	IoMT, integrates and manages many issues related to individuals, including health services, welfare services, and so on. Having all the information about people in one software package can affect the user privacy.	(Afzal et al. 2019; Chen et al. 2014; Khan and Salah 2018; Lee and Lee 2015; Lim et al. 2018; Reyna et al. 2018)
Lack of security and trust management	C_5	The available hardware and software on the IoMT platform are extremely vulnerable due to lack of encryption, insecure web interface and other security issues, and consequently hackers can access all the information on the platform, which creates insecurity for organizations and distrust for individuals.	(Afzal et al. 2019; Farahani et al. 2018; Kamali et al. 2018; Khan and Salah 2018; Khan and Turowski 2016; Kumar and Mallick 2018; Lee and Lee 2015; Makhdoom et al. 2019; Nasrollahi and Ramezani 2020; Reyna et al. 2018)
Intra-organizational resistance (Labor)	C_6	The predominance of traditional approaches to processes, the feeling of job insecurity and also the lack of acceptance of technology-based approaches by the organization cause their high resistance and challenge the dominance of the IoMT platform over the organization.	(Furnell et al. 2009)
Integration of information system of external partners	C_7	Business cooperation of organizations together to achieve sustainable competitive advantage requires integration between their information systems. Business partners have information systems with different processes since data integration from different information systems with different programming languages requires an integrated data system.	(Cooper and James 2009; Furnell et al. 2009)
Cost	C_8	Implementing IoMT is a costly project that companies are reluctant to invest in due to the lack of transparency of the results and also the lack of cost-benefit analysis.	(Afzal et al. 2019; Furnell et al. 2009; Kumar and Mallick 2018)
Technical and empirical knowledge of management and staff	C_9	Since IoMT is an emerging and novel phenomenon, management and staff may not have mastered the relevant technical knowledge, which in turn leads to disruption and sometimes resistance. Therefore, technical training of individuals is vital for the implementation of IoMT.	(Furnell et al. 2009; Kamali et al. 2018)

Top management support	C_{10}	For organizations to participate in the implementation of IoMT, there is a need for support and understanding of IoMT and its applications by senior management to make the necessary changes to implement it.	(Furnell et al. 2009; Luthra and Mangla 2018)
Standardization	C_{11}	The IoMT is a network with a large number of heterogeneous devices that meet different standards and must interact with each other. Standardization can improve interoperability and allow products and services to compete at higher levels. However, the rapid growth of the Internet of Things has made it difficult to establish standards including interoperability, accessibility, and security.	(Choudhary, Virmani, and Juneja 2020; Kamali et al. 2018; Kumar and Mallick 2018; Kumar, Vrat, and Shankar 2021; Luthra and Mangla 2018)
Legal Issue	C_{12}	In IoMT, there are no rules on how to use its data, as well as to fight against crimes that occur while using the data; therefore, the security of data and information, as well as the investigation of crimes from a legal point of view must be considered.	(Kumar and Mallick 2018; Luthra and Mangla 2018; Reyna et al. 2018)
The rapid growth of device technology	C_{13}	With the rapid growth of technology, devices and equipment in the IoMT network are becoming more advanced and powerful every day. Therefore, it is necessary that these devices have high flexibility in development or updating so that their replacement and relocation does not impose much cost and time on the organization.	(Luthra and Mangla 2018)

3. Research methodology

The present research is applied in terms of purpose and a descriptive-survey in terms of data collection. In this study, the existing literature studies were used to identify the challenges of IoMT implementation in smart manufacturing, and on the other hand, field studies were conducted to complete the questionnaire. Experts of the present study are manufacturing managers and consultants active in the automotive industry who have work experience in the field of manufacturing and research and applied experience in the field of Internet of Things. The questionnaires were sent to the experts by e-mail and among them 6 questionnaires were completed and returned by the respondents.

In this study, in order to achieve the relationship between the challenges of IoMT and creating a hierarchical structure, after reviewing the literature in this area, the challenges were identified and then, through a questionnaire, the opinions of experts were collected. The ISM technique was used to create a hierarchical structure. Finally, MICMAC analysis was conducted to investigate the driving power and dependence power of the challenges (See Figure (3))

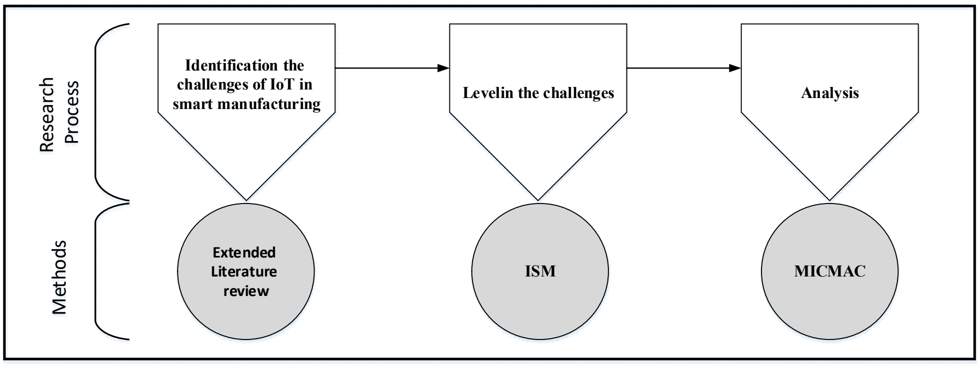

Figure 3. Research Framework

3-1. Interpretive Structural Modeling (ISM)

Interpretive structural modeling is a systematic and structured method introduced by Warfield (1974). ISM is a powerful technique that breaks down a complex system into several subsystems and transforms it into a hierarchical model. This methodology is a combination of three demonstrating languages of words, diagraphs and discrete mathematics (Kaswan and Rathi 2019). ISM is used to determine the interaction between factors as well as to determine the impact of factors (Ali et al. 2022; Yang and Lin 2020). One of the logics of this method is that the factors that have a greater impact on a system than other factors are more important. This technique helps to establish order in the complex relationships between the elements of a system (Agarwal et al., 2007). It can also prioritize and level the elements of a system, which helps managers to have a better execution of the designed model. ISM technique in various fields such as lean Six Sigma enablers (Kaswan and Rathi 2019) 2019), green building project risks (Guan et al. 2020), the study of supply chain sustainability (Chand, Thakkar, and Ghosh 2020), effective factors in green innovation performance (Yang and Lin 2020) and ... has been used.

To perform the interpretive structural modeling technique and obtain the internal relationships and priorities of the elements in a system, six steps must be followed. First the elements/dimensions are determined and then a structural self-interaction matrix is obtained. The initial reachability matrix is then extracted and in the next step the reachability matrix is adapted. Leveling the elements of the reachability matrix is the next step and finally the model is drawn.

Step 1. Formation of structural self-interaction matrix

In this step, a pairwise comparison of the research elements is conducted. For this purpose, the scale presented by Bolaños et al. in 2005 is used, which is shown in Table (3).

Table 3. The proposed scale for the structural self-interaction matrix formation (Bolaños et al. 2005)

Linguistic variables	number
High influence	3
Meduim influence	2
Very low influence	1
No influence	0

Step 2. Creation of initial reachability matrix

At this point, the structural self-interaction matrix becomes a binary matrix. The reachability matrix is obtained by determining the relationships as zero and one from the matrix obtained from the total opinions of the respondents in two steps:

Sub-Step 1: First, a unit numerical scale (m) is considered and the self-interaction matrix numbers are compared with it. Bolanos et al. Defined these relationships as follows:

$$M = \begin{cases} a_{ij} = 1 & if \quad a_{ij} \geq m \\ a_{ij} = 0 & if \quad a_{ij} < m \end{cases}$$

$$m = 2 \times n$$

Where n represents the number of respondents and m represents the value of scale.

Sub-Step 2: In this step, the initial reachability matrix is obtained by adding the results of the first step with unit matrix.

Step 3. Creation of the final reachability matrix

In the next step, the final reachability matrix is formed by applying transitivity relations existing among the variables.

Step 4. Determining relationships and leveling factors

The reachability matrix in step 3 becomes a matrix with a standard framework by placing elements on its levels. In this step, the reachability matrix is categorized into different levels.

To determine the level and priority of variables, a reachability set and an antecedent set are determined for each variable. The reachability set of each variable includes the variables that can be reached through this variable and the antecedent set of each variable includes the variables through which this variable can be reached. This is conducted using the reachability matrix. After determining reachability and antecedent sets for each variable, the intersection set, which includes the shared challenges between the reachability and the antecedent sets, is identified for each variable.

After determining reachability, antecedent, and intersection sets, the level of variables are determined. In the first table, the variable with the same reachability set and intersection set occupy the highest level of the table. After determining this variable or variables, they will be removed from the table and then the next table with the rest of the variables is formed. In the second table, as in the first table, the second-level variable is specified and this process is continued to do so until the level of all variables is determined.

Step 5. Drawing the initial and final interpretive structural model

A structural model is formed using the final reachability matrix. If there is a relationship between factors i and j, this relationship is indicated by an arrow going from i to j, and the ISM model diagram is formed. Finally, after eliminating transferability, the diagram becomes a model based on interpretive structural modeling.

Finally, interpretive structural modeling is created by placing factors according to their level in a directional graph. Factors classified in level one are placed in the lowest hierarchy of interpretive structural modeling model and higher level factors are placed in the higher hierarchy of the model.

3-2. MICMAC Analysis

MICMAC has integrated with the ISM method to help analyze the findings. It is an analysis method that classifies factors into four categories according to their driving power and dependence power. driving power and dependence power are determined using the ISM method. The driving power of a factor is the total number of other factors that are influenced by it, whereas the dependence power of a factor includes the total number of factors that affect it. All factors can be classified into 4 categories (Xu and Zou 2020):

Group 1. Autonomous factors: These factors have weak driving-power and dependence-power. They have few links to the system in which they are located. They cannot affect other factors or be affected by other factors.

Group 2. Dependent factors: These factors have weak driving-power and strong dependence-power. These factors are deeply influenced by linkage factors and driving factors and are less likely to affect other factors.

Group 3. Linkage factors: These factors have strong driving-power and dependence-power, and any change on them will greatly cause the reaction of other factors. In addition, system feedback affects these linkage factors.

Group 4. Driving factors: These factors have strong driving-power but weak dependence-power. These factors greatly affect other factors.

4. Result

In the present study, by reviewing the literature in the field of using the Internet of Things in smart manufacturing, the challenges facing this new manufacturing system have been identified in table (2). Due to the importance of examining the mentioned challenges in the deployment of smart manufacturing and also determining the priority of the challenges to take appropriate measures, their leveling was conducted using ISM.

Based on the defined steps, from the aggregation of experts' opinions, the Structural Self-Interaction Matrix (SSIM) was formed and presented in table (4).

Table 4. Structural Self-Interaction Matrix

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}
C_1	0	1	16	3	2	3	3	16	2	1	2	18	3
C_2	18	0	0	16	3	1	2	3	0	0	1	2	1
C_3	17	17	0	2	1	3	2	17	1	2	1	1	1
C_4	17	2	0	0	17	2	1	1	1	2	2	1	2
C_5	0	1	3	3	0	16	1	1	0	1	1	1	3
C_6	2	3	1	1	16	0	2	0	18	16	0	15	1
C_7	3	2	3	0	2	1	0	18	1	3	13	18	2
C_8	14	1	13	0	0	0	1	0	0	18	0	0	1
C_9	0	1	0	2	1	18	3	0	0	17	2	2	1
C_{10}	2	0	3	1	1	17	1	1	1	0	2	1	1
C_{11}	18	2	1	1	2	0	18	1	1	0	0	2	14
C_{12}	1	2	1	0	17	1	3	3	0	18	3	0	0
C_{13}	3	17	17	2	2	16	1	2	17	0	16	1	0

According to the structural self-interaction matrix and the scale number (m = 12), the initial reachability matrix was calculated (Table (5)).

Table 5. Initial reachability matrix

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}
C_1	1	1	1	0	1	0	0	1	0	1	0	1	0
C_2	1	1	1	1	1	0	0	1	0	0	0	1	0
C_3	1	1	1	1	0	0	0	1	0	1	0	1	0
C_4	1	0	1	1	1	1	0	1	0	0	0	1	0
C_5	0	0	0	0	1	1	0	0	1	1	0	1	0
C_6	0	0	0	0	1	1	0	0	1	1	0	1	0
C_7	1	0	1	0	1	0	1	1	0	1	1	1	1
C_8	1	1	1	0	0	1	0	1	0	1	0	1	0
C_9	0	0	0	0	1	1	0	0	1	1	0	1	0
C_{10}	0	0	0	0	1	1	0	0	1	1	0	1	0
C_{11}	1	1	1	0	0	1	1	1	1	0	1	1	1
C_{12}	0	0	0	0	1	1	0	0	0	1	0	1	0
C_{13}	1	1	1	1	1	1	1	1	1	1	1	1	1

In the next step, the final reachability matrix was formed by applying transitivity relations existing among the challenges. The final reachability matrix is demonstrated in table (6).

Table 6. The final reachability matrix

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	Driving Power
C_1	1	1	1	1	1	1	0	1	1	1	0	1	0	10
C_2	1	1	1	1	1	1	0	1	1	1	0	1	0	10
C_3	1	1	1	1	1	1	0	1	1	1	0	1	0	10
C_4	1	1	1	1	1	1	0	1	1	1	0	1	0	10
C_5	0	0	0	0	1	1	0	0	1	1	0	1	0	5
C_6	0	0	0	0	1	1	0	0	1	1	0	1	0	5
C_7	1	1	1	1	1	1	1	1	1	1	1	1	1	13
C_8	1	1	1	1	1	1	0	1	1	1	0	1	0	10
C_9	0	0	0	0	1	1	0	0	1	1	0	1	0	5
C_{10}	0	0	0	0	1	1	0	0	1	1	0	1	0	5
C_{11}	1	1	1	1	1	1	1	1	1	1	1	1	1	13
C_{12}	0	0	0	0	1	1	0	0	1	1	0	1	0	5
C_{13}	1	1	1	1	1	1	1	1	1	1	1	1	1	13
Dependence Power	8	8	8	8	13	13	3	8	13	13	3	13	3	

As mentioned, each level is identified when the intersection of reachability set and antecedent set equals reachability set. Then the leveled factors are removed and the intersections are re-examined and the next level factors are determined. This algorithm continues until the leveling is conducted completely. The Table (7) provides reachability set, antecedent set and their intersection set as well as the level related to each challenge.

Table 7. Level partitioning of drivers

Challenge	Reachability set	Antecedent set	Intersection set	Level
C_1	2,3,4,5,6,8,9,10,12	2,3,4,7,8,11,13	2,3,4,8	2
C_2	1,3,4,5,6,8,9,10,12	1,3,4,7,8,11,13	1,3,4,8	2
C_3	2,4,5,6,8,9,10,12	1,2,4,7,8,11,13	2,4,8	2
C_4	1,2, 5,6,8,9,10,12	1,2,3,7,8,11,13	1,2,8	2
C_5	6,9,10,12	1,2,3,4,6,7,8,9,10,11,12,13	6,9,10,11	1
C_6	5,9,10,12	1,2,3,4,5,7,8,9,10,11,12,13	6,9,10,11	1
C_7	1,2,3,4,5,6,8,9,10,11,12,13	11,13	11,13	3
C_8	1,2,3,4,5,6,9,10,12	1,2,3,4,7,11,13	1,2,3,4,	2
C_9	5,6,10,12	1,2,3,4,5,6,7,8,10,11,12,13	5,6,9,10,12	1
C_{10}	5,6,9,12	1,2,3,4,5,6,7,8,9, 11,12,13	5,6,9,12	1
C_{11}	1,2,3,4,5,6,7,8,9,10 ,12,13	7,13	7,13	3
C_{12}	5,6,9,10	1,2,3,4,5,6,7,8,9,10,11,13	5,6,9,10,12	2
C_{13}	1,2,3,4,5,6,7,8,9,10,11,12	7,11	7,11	3

According to the leveling performed in the previous step, a graph was formed as shown in figure (4).

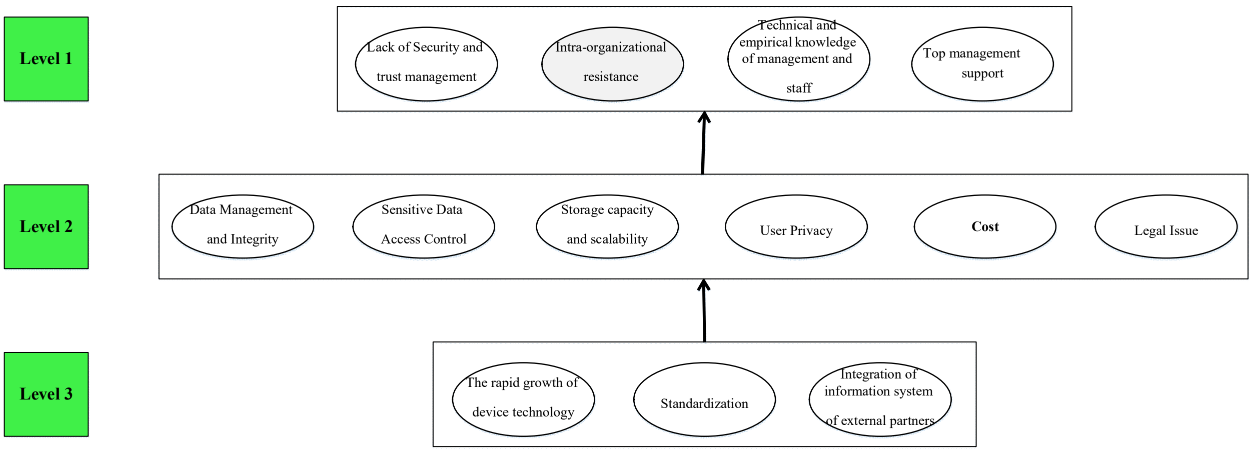

Figure 4. ISM model for Challenges of Internet of Thing in Smart Manufacturing

Conducting MICMAC analysis requires calculating the driving power and the dependence power of each factor, which should be obtained from the summation of each row and the summation of each column in the final reachability matrix, respectively. After calculating these values that are given in table (7), the coordinate figure is illustrated as in Figure (5) where the position of the factors is specified.

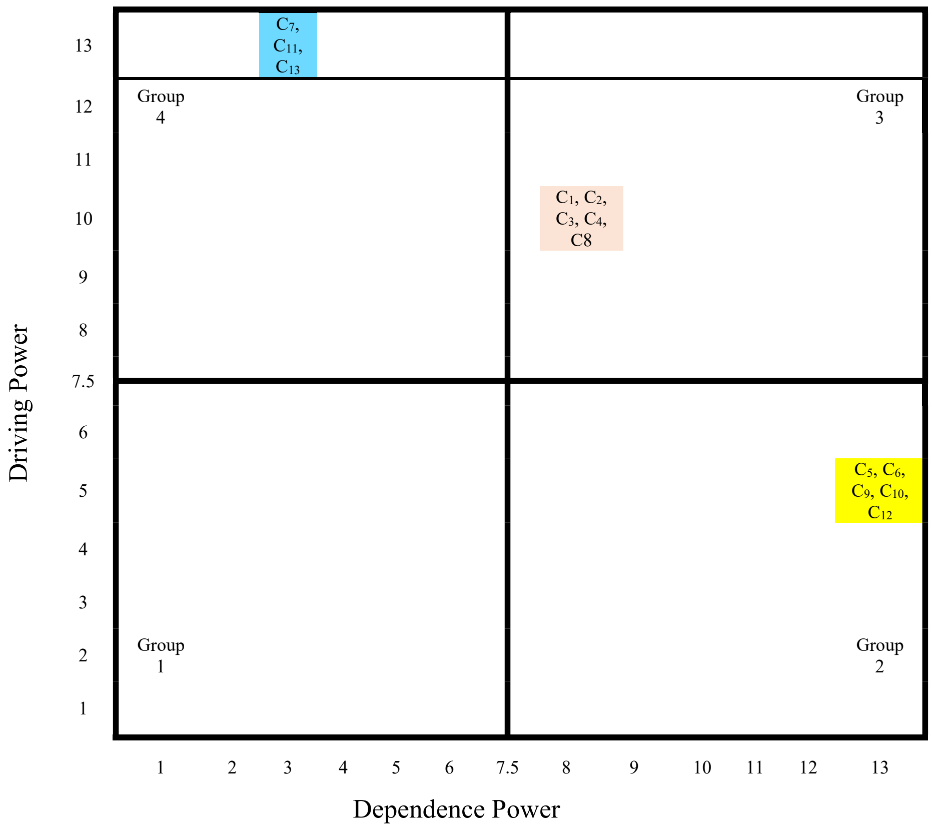

Figure 5. MICMAC Analysis

According to the MICMAC analysis, none of the identified challenges are placed in the group of autonomous factors (group 1), which means that all the challenges introduced are related to the system and affect it. Challenges categorized in Group 2 include lack of security and trust management, Intra-organizational resistance, Technical and empirical knowledge of management and staff, Top management support, and legal issues, which have the potential of highly being influenced (which are highly being influenced). In group 3, there are challenges of data Management and integrity, lack of sensitive data access Control, Storage capacity and scalability, control of access to sensitive data, storage capacity and scalability, privacy, and cost, which are highly interacted with the system. These challenges are highly influential and as well as being highly influenced and consequently much more attention should be focused on them. Integration of information system of external partners, standardization and rapid growth of technology are challenges that have strong driving power that are located in the group of linkage factors (group 4).

5. Discussion

Business relationships with other organizations are recognized as a challenge when they do not have similar information and security systems. In addition, this challenge can occur when multiple organizations with different security and information systems merge with each other (Furnell et al. 2009). Given this challenge, the development of IoMT in smart manufacturing requires a common platform for global standardization. Common standards throughout the world can enable relationships between organizations with other organizations and the integration of organizations al around the world. Addressing these two challenges can help remove the next level challenges, including data management and integration. Another challenge at the third level is that technology is evolving rapidly that is too costly. Therefore, this issue will lead to a cost challenge, which will be addressed at the later level.

The data collected in the system are different, which makes them difficult to manage and integrate. On the other hand, due to the sharing of sensitive data related to inventories, bottlenecks and various incidents, the implementation of IoMT requires updated approaches in the ethical, technical and legal fields. Considering these issues is essential in preventing cyber criminalities because companies are not only responsible for the security of their data but also the data security of supply chain partners (Luthra and Mangla 2018). Another challenge of the second level, which is privacy, will be largely addressed by considering legal issues. Another important issue in implementing IoMT is that all new systems cost a lot of money due to the transformation of all aspects of existing systems. Therefore, investing in new projects requires the acceptance and support given by top management and this is a challenge that will be addressed at level one.

In the implementation and deployment of any new system, top management support is one of the primary key factors and not addressing this organizational factor will create a major challenge in its acceptance and implementation (Luthra and Mangla 2018). Because other factors required to implement a new project such as capital, human labor and equipment are under the control of senior management in the organization. The technical and empirical knowledge of management and staff, in addition to helping them gain support for accepting the deployment of a smart system, will also be a reinforcing factor in the implementation process, as individuals can share their knowledge and experience with others (Furnell et al. 2009). Since human resources play an important role in the implementation and advancement of a new project in the organization, addressing this factor in using IoMT is of vital importance as it can prevent other challenges. Perhaps the lack of a culture of using new information systems can be considered one of the main reasons for intra-organizational resistance within the organization). Using the same user account is not acceptable for employees (Furnell et al. 2009), 2009) and will lead to mistrust, which is another level-one challenge. The resulting feeling of insecurity and mistrust prevents employees from cooperating in the implementation of IoMT in production systems (Afzal et al. 2019).

6. Conclusion

In recent years, the use of the Internet of Things in various aspects of business has attracted the attention of many researchers and industrialists. One of the applications of the Internet of Things is in smart manufacturing. Implementing IoMT in manufacturing, like all new and emerging technologies, will be associated with challenges that are critical to be identified and addressed. Furthermore, it will be vitally important to know which challenges come first and have the greatest impact on the implementation of the smart manufacturing system. Therefore, in this study, by reviewing the literature, the challenges of IoMT implementation in smart manufacturing were identified and in order to determine their importance and level in the automotive industry, the ISM technique was used. According to the opinions of experts in automotive industry and ISM technique, the challenges were classified into three levels. Afterwards, using MICMAC analysis, it was found that among the challenges introduced, the integration of information systems of external partners, standardization and the rapid growth of technology have strong driving power and on the other hand, lack of security and trust management and top management support are highly influenced compared with other challenges.

It seems that due to the emergence of smart manufacturing, it includes various dimensions that can attract researchers interested in this field. The role of human labor in smart manufacturing, the study of technologies required in production processes and the role of intelligence in sustainability are among the issues that can be addressed.

7. References

Afzal, Bilal, Muhammad Umair, Ghalib Asadullah Shah, and Ejaz Ahmed. 2019. "Enabling IoT Platforms for Social IoT Applications: Vision, Feature Mapping, and Challenges." Future Generation Computer Systems 92:718–31. doi: 10.1016/j.future.2017.12.002.

Ali, Sikandar, Jiwei Huang, Samad Baseer, Irshad Ahmed Abbasi, Bader Alouffi, and Wael Alosaimi. 2022. "Analyzing the Interactions among Factors Affecting Cloud Adoption for Software Testing : A Two-Stage ISM-ANN Approach." Soft Computing 26(16):8047–75. doi: 10.1007/s00500-022-07062-3.

Bolaños, Ricardo, Emilio Fontela, Alfredo Nenclares, and Pablo Pastor. 2005. "Using Interpretive Structural Modelling in Strategic Decision-Making Groups." Management Decision 43(6):877–95. doi: 10.1108/00251740510603619.

Chand, Pushpendu, Jitesh J. Thakkar, and Kunal Kanti Ghosh. 2020. "Analysis of Supply Chain Sustainability with Supply Chain Complexity, Inter-Relationship Study Using Delphi and Interpretive Structural Modeling for Indian Mining and Earthmoving Machinery Industry." Resources Policy 68(February):101726. doi: 10.1016/j.resourpol.2020.101726.

Chen, Shanzhi, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang. 2014. "A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective." IEEE Internet of Things Journal 1(4):349–59. doi: 10.1109/JIOT.2014.2337336.

Choudhary, T., C. Virmani, and D. Juneja. 2020. Convergence of Blockchain and IoT: An Edge Over Technologies. Vol. 846. Springer International Publishing.

Cooper, Joshua, and Anne James. 2009. "Challenges for Database Management in the Internet of Things." IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India) 26(5):320–29. doi: 10.4103/0256-4602.55275.

Dhumale1, R. B., N. D. Thombare, and P. M. Bangare. 2017. "Smart Supply Chain Management Using Internet of Things." International Research Journal of Engineering and Technology (IRJET) 04(06):787–91. doi: 10.1504/IJSCC.2018.090754.

Dorsemaine, Bruno, Jean Philippe Gaulier, Jean Philippe Wary, Nizar Kheir, and Pascal Urien. 2016. "Internet of Things: A Definition and Taxonomy." Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies 72–77. doi: 10.1109/NGMAST.2015.71.

Ebrahimi, Mojtaba, Armand Baboli, and Eva Rother. 2019. "The Evolution of World Class Manufacturing toward Industry 4.0: A Case Study in the Automotive Industry." IFAC-PapersOnLine 52(10):188–94. doi: 10.1016/j.ifacol.2019.10.021.

Edgar, Thomas F., and Efstratios N. Pistikopoulos. 2018. "Smart Manufacturing and Energy Systems." Computers and Chemical Engineering 114:130–44. doi: 10.1016/j.compchemeng.2017.10.027.

Farahani, Bahar, Farshad Firouzi, Victor Chang, Mustafa Badaroglu, Nicholas Constant, and Kunal Mankodiya. 2018. "Towards Fog-Driven IoT EHealth: Promises and Challenges of IoT in

Medicine and Healthcare." Future Generation Computer Systems 78:659–76. doi: 10.1016/j.future.2017.04.036.

Furnell, Steven M., Nathan Clarke, Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov. 2009. "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management." Information Management & Computer Security 17(1):4–19. doi: 10.1108/09685220910944722.

Hristov, Kalin. 2017. "Internet plus Policy: A Study on How China Can Achieve Economic Growth through the Internet of Things." Journal of Science and Technology Policy Management 8(3):375–86. doi: 10.1108/JSTPM-03-2017-0007.

Kamali, Ali, Saeed Ghafoori, Ayoub Mohammadian, Reza Mohammadkazemi, Bahareh Mahbanooei, and Rohollah Ghasemi. 2018. "A Fuzzy Analytic Network Process (FANP) Approach for Prioritizing Internet of Things Challenges in Iran." Technology in Society 1–11. doi: 10.1016/j.techsoc.2018.01.007.

Kaswan, Mahender Singh, and Rajeev Rathi. 2019. "Analysis and Modeling the Enablers of Green Lean Six Sigma Implementation Using Interpretive Structural Modeling." Journal of Cleaner Production 231:1182–91. doi: 10.1016/j.jclepro.2019.05.253.

Khan, Ateeq, and Klaus Turowski. 2016. "A Survey of Current Challenges in Manufacturing Industry and Preparation for Industry 4.0." Pp. v–vi in Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry"(IITI'16) (pp. 15-26). Vol. 451. Cham: Springer.

Khan, Minhaj Ahmad, and Khaled Salah. 2018. "IoT Security: Review, Blockchain Solutions, and Open Challenges." Future Generation Computer Systems 82:395–411. doi: 10.1016/j.future.2017.11.022.

Khan, Shahbaz, Mohd Imran Khan, and Abid Haleem. 2020. "Prioritisation of Challenges Towards Development of Smart Manufacturing Using BWM Method. In Internet of Things (IoT)." Pp. 409–26 in Springer.

Kouicem, Djamel Eddine, Abdelmadjid Bouabdallah, and Hicham Lakhlef. 2018. "Internet of Things Security: A Top-down Survey." Computer Networks 141:199–221. doi: 10.1016/j.comnet.2018.03.012.

Krasniqi, X., and E. Hajrizi. 2016. "Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles." IFAC-PapersOnLine 49(29):269–74. doi: 10.1016/j.ifacol.2016.11.078.

Kumar, Nallapaneni Manoj, and Pradeep Kumar Mallick. 2018. "Blockchain Technology for Security Issues and Challenges in IoT." Procedia Computer Science 132:1815–23. doi: 10.1016/j.procs.2018.05.140.

Kumar, Veepan, · Prem Vrat, and Ravi Shankar. 2021. Prioritization of Strategies to Overcome the Barriers in Industry 4.0: A Hybrid MCDM Approach. Springer India.

Lanotte, Ruggero, and Massimo Merro. 2018. "A Semantic Theory of the Internet of Things." Information and Computation 259(Coordination 2016):72–101. doi: 10.1016/j.ic.2018.01.001.

Lee, In, and Kyoochun Lee. 2015. "The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises." Business Horizons 58(4):431–40. doi: 10.1016/j.bushor.2015.03.008.

Lee1, Gyu Myoung, Noel Crespi1, Jun Kyun Choi, and Matthieu Boussard. 2013. "LNCS 7768 - Internet of Things." Lncs 7768:257–82.

Li, Shaobo, Weixing Chen, Jie Hu, and Jianjun Hu. 2018. "ASPIE : A Framework for Active Sensing and Processing of Complex Events in the Internet of Manufacturing Things." doi: 10.3390/su10030692.

Lim, Chiehyeon, Kwang Jae Kim, and Paul P. Maglio. 2018. "Smart Cities with Big Data: Reference Models, Challenges, and Considerations." Cities 82(February):86–99. doi: 10.1016/j.cities.2018.04.011.

Liu, Jing, Yang Xiao, Shuhui Li, Wei Liang, and C. L. Phili. Chen. 2012. "Cyber Security and Privacy Issues in Smart Grids." IEEE Communications Surveys and Tutorials 14(4):981–97. doi: 10.1109/SURV.2011.122111.00145.

Luthra, Sunil, and Sachin Kumar Mangla. 2018. “Evaluating Challenges to Industry 4.0 Initiatives for Supply Chain Sustainability in Emerging Economies.” Process Safety and Environmental Protection 117:168–79. doi: 10.1016/j.psep.2018.04.018.

Makhdoom, Imran, Mehran Abolhasan, Haider Abbas, and Wei Ni. 2019. “Blockchain’s Adoption in IoT: The Challenges, and a Way Forward.” Journal of Network and Computer Applications 125:251–79. doi: 10.1016/j.jnca.2018.10.019.z

Nasrollahi, Mahdi, and Javaneh Ramezani. 2020. “A Model to Evaluate the Organizational Readiness for Big Data Adoption.” International Journal of Computers, Communications and Control 15(3):1–11. doi: 10.15837/IJCCC.2020.3.3874.

Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. 2018. “On Blockchain and Its Integration with IoT. Challenges and Opportunities.” Future Generation Computer Systems 88(2018):173–90. doi: 10.1016/j.future.2018.05.046.

Rose, Kenneth A., Shaye Sable, Donald L. DeAngelis, Simeon Yurek, Joel C. Trexler, William Graf, and Denise J. Reed. 2015. “Proposed Best Modeling Practices for Assessing the Effects of Ecosystem Restoration on Fish.” Ecological Modelling 300:12–29. doi: 10.1016/j.ecolmodel.2014.12.020.

Xu, Xiaoxiao, and Patrick X. W. Zou. 2020. “Analysis of Factors and Their Hierarchical Relationships Influencing Building Energy Performance Using Interpretive Structural Modelling (ISM) Approach.” Journal of Cleaner Production 272:122650. doi: 10.1016/j.jclepro.2020.122650.

Xu, Yongzhao, Renato W. R. De Souza, Elias P. Medeiros, Neha Jain, Lijuan Zhang, Leandro A. Passos, and Victor Hugo C. De Albuquerque. 2022. “Intelligent IoT Security Monitoring Based on Fuzzy Optimum-Path Forest Classifier.” Soft Computing. doi: 10.1007/s00500-022-07350-y.

Yang, Zhan, and Yun Lin. 2020. “The Effects of Supply Chain Collaboration on Green Innovation Performance:An Interpretive Structural Modeling Analysis.” Sustainable Production and Consumption 23:1–10. doi: 10.1016/j.spc.2020.03.010.

Zhang, Yingfeng, Wenbo Wang, Sichao Liu, and Gongnan Xie. 2014. “Real-Time Shop-Floor Production Performance Analysis Method for the Internet of Manufacturing Things.” 2014. doi: 10.1155/2014/270749.

Zhuming Bi, Li Da Xu, and Chengen Wang. 2014. “Internet of Things for Enterprise Systems of Modern Manufacturing.” IEEE Transactions on Industrial Informatics 10(2):1537–46. doi: 10.1109/TII.2014.2300338.