ISSN: 2783-2678

International journal of Innovation in Management Economics and Social Sciences

Journal homepage: www.ijimes.ir

Int. J. Inn. Man. Eco. Soc. Sci. Vol. 3, No, 2, 1-12.

Security and privacy analysis based on Internet of Things in the fourth industrial generation (Industry 4.0)

Mahmonir Bayanati[1,*]

[1] *Department of Management, Islamic Azad University, West Tehran Branch, Tehran, Iran*

ARTICLE INFO

Received:15 January 2023

Reviewed:5 February 2023

Revised: 20 February 2023

Accept: 1 April 2023

Keywords: Internet of Things, Industry 4.0, privacy, security of Internet of Things, Industrial Internet of Things (IIoT)

ABSTRACT

The connection of smart devices using the Internet has dramatically changed the way people live, and this concept has also been extended to the industrial sector. This practice not only provides more stable, faster, and safer communications but also makes it possible to realize the concept of the smart factory in the fourth industrial revolution. The Internet of Things uses a unique Internet Protocol to identify, control, and transmit data to individuals as well as databases. Data is collected through the Internet of Things, stored in cloud storage, and managed and calculated through analytical tools. Internet of Things security is a field of technology that focuses on protecting connected devices and networks in the Internet of Things (IoT). Ensuring the safety of networks with connected IoT devices is critical. Security in the Internet of Things includes a wide range of techniques, strategies, protocols, and measures aimed at mitigating the ever-increasing vulnerabilities of the Internet of Things in modern businesses. The simultaneous connection of objects also brings privacy concerns. For this reason, in this research, an effort has been made to examine and analyze the most important privacy requirements in the Internet of Things in digital businesses in Industry 4.0. In this regard, by using experts' opinions and literature review, privacy requirements were extracted and evaluated using fuzzy non-linear decision-making methodology. The results showed that acquired and intrinsic information has the highest importance.

[*] Corresponding Author: Mahmonir@gmail.com

1. Introduction

Business leaders understand that long-term success in the new era requires new ways of thinking and acting in the face of rapid global economic and technological change. In fact, companies are rewriting and replacing another program that takes business capabilities to a level never seen before. In this aggressive environment, fostering innovation is the most important strategic priority of industries. The Internet of Things has changed business practices globally, and the manufacturing industry is no exception [1]. By combining the real and virtual world and production through the Internet, the Internet of Things provides the possibility of connecting all parts of the production process (machines, materials, people, etc.) [2].

The main idea of the Internet of Things is a system in which physical items are equipped with embedded electronic components (RFID tags, sensors, etc.), and are connected to the Internet; Therefore, the Internet of Things relies on both smart objects and smart networks. Thanks to the Internet of Things, physical objects are seamlessly integrated into the information network, where they can be used in business processes [3]. They share information about their condition, the surrounding environment, production processes, maintenance schedule and even other things with each other. The industry standard 4.0 is part of the fourth industrial revolution, which includes the Internet of Things, machines, computers, and people that perform intelligent industrial operations using advanced data analytics to transform business outcomes that are redefining the landscape [4]. It is for businesses and individuals. Industry 4.0 framework, also known as the smart factory, is connected with sensors and smart digital devices and they communicate intelligently with each other. It is the relationship between raw material, semi-finished product, tool, robot, etc. Industry 4.0 framework and standard has more flexibility, optimal use of resources and integration of customers and business partners in the business process [5].

Since the Internet of Things is so broad, the security of the Internet of Things is much broader than the Internet of Things itself. This has led to various methods falling under the umbrella of IoT security. Application Program Interface (API) security, Public Key Infrastructure (PKI) authentication, and network security are just a few of the methods IT managers can use to combat the growing threat of cybercrime and cyberterrorism rooted in vulnerable IoT devices [6].

The more ways there are to connect devices to each other, the more threat actors can intercept them. Protocols such as HTTP (Hypertext Transfer Protocol) and API are just a few of the channels that IoT devices rely on and can be intercepted by hackers. The IoT umbrella strictly includes only Internet-based devices. Appliances that use Bluetooth technology are also considered IoT devices and therefore require IoT security. Such oversights have contributed to the recent surge in IoT-related data breaches [7]. The problem of privacy is very important among the security aspects of the Internet of Things, because the failure to protect privacy causes the system and services of the Internet of Things not to be accepted by different people and organizations, as a result of which the final goal is lost [8]. The category of privacy is much more vital in the Internet of Things. Unlike the normal Internet, the amount of information measured in the Internet of Things (from people or by people) is much higher, and therefore the risk of revealing personal information of people will be much higher [9].

According to the cases raised in this research, it has been tried to investigate and analyze the privacy requirements in the Internet of Things by emphasizing the literature review and experts' opinions. In order to analyze the data, a hierarchical decision-making method based on AHP is used. The results will provide a correct understanding of privacy requirements in the Internet of Things.

The structure of the research is as follows. In the second part, the literature review is presented and the most important privacy requirements in the Internet of Things are introduced. In the third part, the research method is presented, and in the fourth part, the research results are presented, and finally, the conclusion and discussion are presented in the last part.

2. Literature Review

IoT is defined as a network of physical objects. The Internet consists not only of computers but also of various devices such as smart phones, home appliances, people, etc., which are all shared and connected through the Internet and used to achieve monitoring, online upgrading, and intelligent management [10]. IIoT or Industrial Internet of Things usually refers to sensors, instruments and other interconnected devices that are connected in an industrial environment. This connectivity enables remote access and monitoring, but most importantly, it enables data acquisition and collection, exchange and analysis of various data sources. This has huge potential to improve productivity and efficiency [11]. IIoT solutions are described as being cost effective and quick to implement.

Anything connected to the Internet is likely to be attacked at some point. Attackers can remotely compromise IoT devices using various methods. These devices are connected to the system of computing devices, mechanical and digital machines and any objects that can exchange or collect data for monitoring and control. When attackers gain control of the IoT, they can use it to steal data, conduct distributed denial-of-service (DDoS) attacks, or compromise other connected networks [12].

Stakeholders play an important role in ensuring security in the Internet of Things. Device manufacturers must design the device hardware to be attack resistant. Software programmers must write high security code to run on devices. Engineers responsible for deploying and managing IoT devices are required to take necessary measures to reduce security risks [13, 14]. end users accessing data or systems through the Internet of Things; They should keep devices safe and avoid unauthorized access to users. IoT devices are subject to inherent security challenges and vulnerabilities. IT security teams should review the following operations [15]:

- Ensuring the vulnerability and correctness of software updates running on IoT devices
- Protecting the vulnerability of communication APIs in IoT devices
- Monitoring the penetration of Internet networks
- Securely store data collected on IoT devices or uploaded to the data center

Figure 1 shows some examples of the challenges of the Internet of Things in the field of security [16].

- One of the most important challenges of the Internet of Things in terms of security is the risk of shadow devices or devices that are connected to the Internet of Things network but are not authorized or recognized by the network owner [17].
- IoT systems are often not properly updated to protect against security vulnerabilities. IoT devices are usually small and deployed in remote locations. An organization may have thousands of IoT devices to manage, so it is possible for organizations to forget where their IoT devices are located.
- Exchanging data over the network via an application programming interface (API) is only a small part of what IoT devices do. Vulnerabilities in APIs are a significant security risk.

- Many IoT devices have default passwords that allow users to access software environments within the systems.
- Because there is no single IoT API, there is no single standard to control the design of IoT systems, the types of software they run, or how data is exchanged.

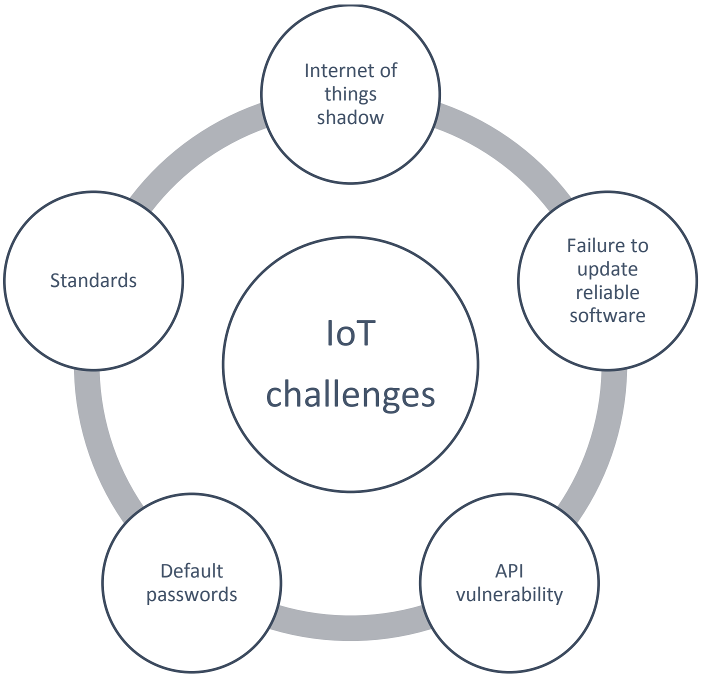
Internet of things shadow
Failure to update reliable software
IoT challenges
Standards
Default passwords
API vulnerability

Fig. 1. Challenges of the Internet of Things.

2.1. Security and privacy in the Internet of Things

With the advent of the Internet, the way people communicate with each other underwent a fundamental revolution [18]. The second wave of Internet development will no longer be about humans, but about intelligent connected devices. Although more than a decade has passed since the concept of "Internet of Things" was introduced, the development of this concept has been slow due to various reasons such as the lack of development of the required technologies and the existence of security challenges [19]. Connecting industrial machines to Internet of Things networks increases the risk of hackers discovering and attacking these devices. Industrial espionage or a malicious attack on critical infrastructure are both irreparable risks. This means that businesses must ensure that these networks are isolated and protected, and data encryption is essential to secure sensors, and other components [20].

In computing systems, the core security concerns are related to the information used by the system. Citizens' right to privacy is intertwined with the challenge of cyber security and the interests of the smart city. The legal/social concept of privacy refers to the confidential aspects of life, control of its public profile and a life free from undue interference [21]. Necessary measures to ensure the architecture's resilience to attacks, data authentication, access control and customer privacy. must be done A suitable legal framework in this technology should exist and be established in the best way by the international legislator to be supported by the private sector according to specific needs [22].

The widespread adoption of wireless media for information exchange causes the publication and development of new topics in the field of privacy violations. In fact, wireless networks, due to their remote access capability, increase the risk of privacy violations because they make the system vulnerable to potential eavesdropping and masking attacks [23]. Therefore, privacy protection represents a real issue that may limit the development of the Internet of Things. The findings suggest that (a) applications do not adequately protect the personal privacy of data collected through the Internet of Things, and (b) future privacy laws should address the consequences of universal access to Internet of Things services [24]. and consider the ubiquity and security of data collection of the Internet of Things with respect to people's privacy [25].

Considering the above and also the limited financial and human resources, the cost and time that must be spent to compensate for the damage caused by the security holes in the Internet of Things technology and even the life injuries that may be caused by the lack of attention and understanding of security issues in this field, it is necessary to identify and address security issues and challenges in this field [26]. In this research, it has been tried to identify the most important privacy requirements in the Internet of Things by reviewing the literature. After selecting the initial requirements, active experts were asked to refine these requirements. These experts were selected from among the Internet of Things activists who had relevant work records and academic experts with relevant research records [27]. A total of 16 experts were asked. Table 1 shows the requirements of privacy in the Internet of Things taken from the literature review and experts' opinions [28].

Table 1. Privacy requirements in the Internet of Things.

Systematic	Protection of personal information Digital oblivion Preservation of privacy and anonymity Privacy compatibility of different systems Protect privacy while searching The impossibility of tracking the activities of one object by another object
Strategic	Ensuring non-disclosure of data ownership Providing the necessary policies and framework to protect privacy Creating protocols and algorithms for hiding people's private information

- Protection of personal information (acquired and inherent information) is done in order to prevent their leakage.
- Digital oblivion refers to ensuring that personal information is deleted after use.
- Privacy and anonymity (allowing the use of pseudonyms in certain circumstances) are used for heterogeneous sets of devices (provided by digital identity management).
- Protecting privacy while searching refers to the discovery of Internet of Things services and devices.
- The impossibility of tracking the activities of one object by another object indicates the tracking based on the integrity of information devices.

- It is very important to ensure that the ownership of data, devices and objects are not disclosed to unauthorized people [29].
- Providing the necessary policies and framework to protect privacy and registering the laws related to it is a basic duty that should be given high attention in policy making.
- It is very important to create protocols and algorithms that hide people's private information, such as face or location (so that only authorized people can open it).
- Networks provide a huge opportunity for threat actors to remotely control other people's IoT devices. Since networks include both digital and physical components, indoor IoT security must address both types of access points.

3. Research method

Traditional hierarchical analysis, which has been used so far, requires accurate judgments. But due to the complexity and uncertainty of real decision-making issues, it is often unrealistic or even impossible to provide accurate judgments. Therefore, it is much more realistic and practical if this possibility can be provided to the decision maker to use inaccurate judgments using fuzzy logic instead of accurate judgments. In 2004, Mikhailov [30] presented a new approach to calculate weights in the fuzzy AHP method, and he called this method fuzzy prioritization. One of the most important features of this method is the calculation of the compatibility rate in the fuzzy state.

In this method, it is assumed that fuzzy pairwise comparisons are triangular fuzzy numbers. The deterministic vector of weight (priority) $\mathrm{w} = (\mathrm{w}_1, \mathrm{w}_2, \dots, \mathrm{w}_\mathrm{n})$ is extracted in such a way that the priority rate is almost within the range of the basic fuzzy judgments. In other words, the weights are determined in such a way that the following relationship is established.

$$l_{ij} \overset{\sim}{\leq} \frac{w_i}{w_j} \overset{\sim}{\leq} u_{ij} \qquad (1)$$

Any deterministic weight vector (w) with a degree applies to the above fuzzy inequalities, which can be measured through the linear membership function of the following relationship (in terms of the unknown rate):

$$\mu_{ij}\left(\frac{w_i}{w_j}\right) = \begin{cases} \dfrac{(w_i / w_j) - l_{ij}}{m_{ij} - l_{ij}} & \dfrac{w_i}{w_j} \leq m_{ij} \\ \dfrac{u_{ij} - (w_i / w_j)}{u_{ij} - m_{ij}} & \dfrac{w_i}{w_j} \leq m_{ij} \end{cases} \qquad (2)$$

Considering the specific form of the membership functions, the fuzzy prioritization problem becomes a nonlinear optimization problem as follows.

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

Considering the non-linearity of the relationship (3), it is obvious that it is not possible to solve it without using the software. Therefore, GAMS software was used to solve the models created in this research. Positive optimal values for index λ (objective function) it indicates that all the ratios of weights apply completely in the initial judgment, but if this index is negative, it can be understood that the fuzzy judgments are strongly inconsistent and the ratios of weights are almost applied in these judgments.

4. Research method

The process related to the ranking of the key indicators of the evaluation of Privacy requirements in the Internet of Things in this study is divided into two main parts:

1- Determining the matrix of pairwise comparisons based on the integration of experts' opinions
2- Using mathematical modeling in order to rank and obtain the weight of indicators in the research model.

In order to prioritize the 9 final needs extracted in this research, fuzzy questionnaires using language variables were sent to 16 experts and university professors. 13 questionnaires were completed and received. These pairwise comparison tables are shown in tables (2) to (4). These tables were used for calculations using the Mikhailov method.

Table 2. Pairwise comparison matrix for general classification (systematic and strategic).

	W1			W2		
W1	-	-	-	-	-	-
W2	1.75	2.45	4.2	-	-	-

Table 3. Pairwise comparison matrix for systematic needs.

	W11			W12			W13			W14			W15			W16		
W11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
W12	1.25	2.25	3.21	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
W13	2.1	3.1	4.8	2.1	2.5	3.5	-	-	-	-	-	-	-	-	-	-	-	-
W14	1.75	2.8	4.1	2.25	3.25	4.25	1.2	2.4	3.8	-	-	-	-	-	-	-	-	-
W15	1.1	2.87	3.78	1.78	2.75	3.78	1.1	3.5	4.2	2.25	3.11	4.5	-	-	-	-	-	-
W16	1.25	1.75	3.1	2.1	2.75	2.98	1.87	2.5	3.6	1.78	2.45	3.1	1.1	2.5	3.1	-	-	-

Table 4. Pairwise comparison matrix for strategic needs.

	W21			W22			W23		
W21	-	-	-	-	-	-	-	-	-
W22	1.25	2.7	4.2	-	-	-	-	-	-
W23	1.2	3.1	3.9	2.2	3.25	4.75	-	-	-

By placing the data obtained from tables number (2) to (4) in the non-linear model (3) as a model providing weights and ranks based on hierarchical analysis and solving the model using GAMS software, the weight, and rank can be Each of the evaluation indicators was obtained in general dimensions as well as in exclusive categories. The calculation results related to solving the non-linear model for general categories and individual indicators are shown in tables (5) to (7).

Table 5. Weight and ranking of the main categories.

Category	Code	Weight	Rank	The objective function(λ)
Systematic	W1	0.65412	1	0.38471
Strategic	W2	0.34588	2	

Table 6. Weight and ranking of the systematic categories.

Category	Code	Weight	Rank	The objective function(λ)
Protection of personal information	W11	0.29124	1	0.53214
Digital oblivion	W12	0.21785	3	
Preservation of privacy and anonymity	W13	0.25417	2	
Privacy compatibility of different systems	W14	0.07874	5	
Protect privacy while searching	W15	0.10425	4	
The impossibility of tracking the activities of one object by another object	W16	0.05212	6	

Table 7. Weight and ranking of the strategic categories.

Category	Code	Weight	Rank	The objective function(λ)
Ensuring non-disclosure of data ownership	W21	0.32154	2	0.49857
Providing the necessary policies and framework to protect privacy	W22	0.49148	1	
Creating protocols and algorithms for hiding people's private information	W23	0.18421	3	

As it can be seen in tables (5) to (7), a positive value for the compatibility index indicates acceptable compatibility of the matrices. After obtaining the weight of the general categories and the weight of the indicators in specific categories, we can normalize the weights and get the total weight of all the indicators. without considering the category and also their overall rank. The normalized calculation results are shown in Table number (8).

Table 8. Normal weight and final ranking of requirements.

Category	Weight	Requirements	Weight	Normal weight	Rank
systematic	0.65412	Protection of personal information	0.29124	0.190506	1
		Digital oblivion	0.21785	0.1425	4
		Preservation of privacy and anonymity	0.25417	0.166258	3
		Privacy compatibility of different systems	0.07874	0.051505	8
		Protect privacy while searching	0.10425	0.068192	6
		The impossibility of tracking the activities of one object by another object	0.05212	0.034093	9
strategic	0.34588	Ensuring non-disclosure of data ownership	0.32154	0.111214	5
		Providing the necessary policies and framework to protect privacy	0.49148	0.169993	2
		Creating protocols and algorithms for hiding people's private information	0.18421	0.063715	7

As can be seen in Table 8, Protection of personal information has the highest rank among security and privacy requirements in the Internet of Things. Therefore, this requirement is one of the main priorities and solutions should always be considered to respond to this requirement. Figure ٢ shows the normalized weights for these requirements.

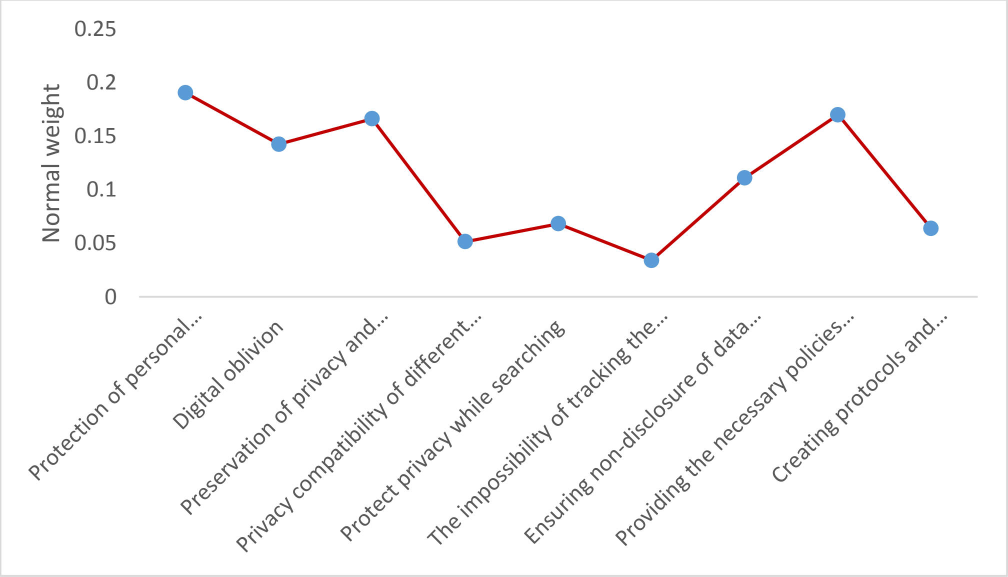

Fig. 2. Normalized weights for privacy requirements in the Internet of Things.

This analysis shows that there is still no high concern about the impossibility of tracking the activities of one object by another object or it has a lower priority.

5. Conclusion

With the advent of the Internet, the way people communicate with each other underwent a fundamental revolution. The second wave of Internet development will no longer be about humans, but about intelligent connected devices. Although more than a decade has passed since the concept of "Internet of Things" was introduced, the development of this concept has been slow due to various reasons such as the lack of development of the required technologies and the existence of security challenges. When we are researching smart environments and technologies such as the Internet of Things, we must spend extra time and energy to understand security challenges and existing solutions. The security of the Internet of Things is actually a specific part of the field of technology that focuses on the protection of devices and networks connected to the Internet of Things and includes various equipment, including mechanical and digital machines, computing devices, technologies such as artificial intelligence, etc. did All these things are connected to each other through the Internet and the Internet is always exposed to various risks, including hacking and unauthorized access to information. This is why security in the Internet of Things is of great importance. IoT makes computing physical, that is, it has a physical layer that has sensors to sense and collect information about the environment and use the information given by these sensors for similar environments, so if things go wrong with IoT devices, it can have major consequences in have real world. Connecting to the Internet also means connecting to potential cyber threats. Cyber security is an area that every business should pay attention to. Unfortunately, the number of companies that have a plan to deal with this threat is woefully small. The biggest problem is that most companies believe limited protection will save them.

Considering the importance of security and privacy in the Internet of Things, this research tried to evaluate and analyze the security aspects of the Internet of Things in Industry 4.0. Therefore, for this purpose, the most important privacy requirements were identified by reviewing the literature. Then, using the opinions of experts, these requirements were refined and the most important requirements were extracted. Experts were selected from among the activists in the fields of information technology and Internet of Things with suitable work records, as well as academic experts with relevant research records. In order to analyze the data from the method Fuzzy nonlinearity was used. The results show that Protection of personal information has the highest priority among the privacy requirements in the Internet of Things and special attention should be paid to it.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The author declares no conflict of interest related to this publication.

References

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

[2] Douiba, M., Benkirane, S., Guezzaz, A., & Azrour, M. (2023). An improved anomaly detection model for IoT security using decision tree and gradient boosting. The Journal of Supercomputing, 79(3), 3392-3411.

[3] Obaid, H. S., & Nozari, H. (2022). Examining Dimensions and Components and Application of Supply Chain Financing (In Chain Stores). International Journal of Innovation in Management, Economics and Social Sciences, 2(4), 81-88.

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

[5] Abdulsamad, A. A., & Salih, T. A. (2023). IoT security improvement based on SDN Controller. Eurasian Journal of Engineering and Technology, 14, 49-56.

[6] Shayannia, S. A. (2022). Designing a Multiobjective Human Resource Scheduling Model Using the Tabu Search Algorithm. Discrete Dynamics in Nature and Society, 2022.

[7] Fallah, M., Sadeghi, M. E., & Nozari, H. (2021). Quantitative analysis of the applied parts of Internet of Things technology in Iran: an opportunity for economic leapfrogging through technological development. Science and technology policy Letters, 11(4), 45-61.

[8] Aliahmadi, A., Nozari, H., & Ghahremani-Nahr, J. (2022). AIoT-based sustainable smart supply chain framework. International journal of innovation in management, economics and social sciences, 2(2), 28-38.

[9] Toloie-Eshlaghy, A., & Bayanati, M. (2013). Ranking information system success factors in mobile banking systems with VIKOR. Middle-East Journal of Scientific Research, 13(11), 1515-25.

[10] Nozari, H., & Szmelter-Jarosz, A. (2022). IoT-based Supply Chain For Smart Business (Vol. 1). ISNET.

[11] Eisapour, K., Bayanati, M., & Yousefpour, J. (2013). A mathematical model for ranking R&D organizationsas a technology development factor. Advances in Environmental Biology, 717-721.

[12] Bayanati, M., Toloie-Eshlaghy, A., & Bayanati, M. IS Success in M-Banking Systems: A Dynamic Approach.

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

[14] Bayanati, M., Peivandizadeh, A., Heidari, M. R., Foroutan Mofrad, S., Sasouli, M. R., & Pourghader Chobar, A. (2022). Prioritize Strategies to Address the Sustainable Supply Chain Innovation Using Multicriteria Decision-Making Methods. Complexity, 2022.

[15] Pishkar, N., Nasimi, M. A., & RAHMATI, M. (2021). Developing a Conceptual Model of Green Supply Chain Antecedents and Consequences in the Qualification Approach.

[16] Nozari, H., Szmelter-Jarosz, A., & Ghahremani-Nahr, J. (2022). Analysis of the Challenges of Artificial Intelligence of Things (AIoT) for the Smart Supply Chain (Case Study: FMCG Industries). Sensors, 22(8), 2931.

[17] Rafierad, S., Aghajani, H. A., Agha Ahmadi, G., & Rahmaty, M. (2022). Construction and Validation of Dimensions and Components of the Organizational Anomie Scale in order to provide a Native Model in Government Hospitals. Journal of System Management, 8(2), 57-73.

[18] Salehi Koocheh Baghi, S. A., Rahmaty, M., & Kia Kojouri, D. (2021). Presenting a Model of Organizational Insentience in the Red Crescent Society. Quarterly Scientific Journal of Rescue and Relief, 13(3), 228-236.

[19] Aliahmadi, A., Nozari, H., & Ghahremani-Nahr, J. (2022). Big Data IoT-based agile-lean logistic in pharmaceutical industries. International Journal of Innovation in Management, Economics and Social Sciences, 2(3), 70-81.

[20] Daneshvar, A., Ebrahimi, M., Salahi, F., Rahmaty, M., & Homayounfar, M. (2022). Brent Crude Oil Price Forecast Utilizing Deep Neural Network Architectures. Computational Intelligence and Neuroscience, 2022.

[21] Vakilian Sayyah, M., Aghajani, H. A., Agha Ahmadi, G. A., & Rahmaty, M. (2022). Analyzing dimensions, consequences, and inequalities of organizational citizenship behaviour in non-governmental organizations of crisis management (experimental evidence: Red Crescent Society of the Islamic Republic of Iran). Journal of rescue and relief, 14(3), 163-175.

[22] Nozari, H., Fallah, M., & Szmelter-Jarosz, A. (2021). A conceptual framework of green smart IoT-based supply chain management. International journal of research in industrial engineering, 10(1), 22-34.

[23] Shayan Nia, S. A., Mohammadi, M., Lotfi, M. R., & Rezaeian, J. (2022). Determining the Sequence and Schedule of Job-shop Production Systems using Genetic Algorithm by considering Possible Values. Journal of Industrial Strategic Management, 7(1), 42-51.

[24] Ashok, K., & Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective. IEEE Access, 11, 2621-2651.

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

[26] Alijanzadeh, M. R., Shayannia, S. A., & Movahedi, M. M. (2022). Optimization Of Maintenance In Supply Chain Process And Risk-Based Critical Failure Situations (Case study: Iranian Oil Pipeline And Telecommunication Company, North District). Journal of Applied Research on Industrial Engineering.

[27] Shayannia, S. A. (2023). Presenting an agile supply chain mathematical model for COVID-19 (Corona) drugs using metaheuristic algorithms (case study: pharmaceutical industry). Environmental Science and Pollution Research, 30(3), 6559-6572.

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

[29] Keliji, P. B., Aghajani, H. A., Movahedi, M. M., & Shayannia, S. A. (2022). The Analysis of the Role of Bullwhip Effects on the Four-Level Supply Chain in Industry Using Statistical Methods. Discrete Dynamics in Nature and Society, 2022.

[30] Nozari, H., Sadeghi, M. E., & Najafi, S. E. (2022). Quantitative Analysis of Implementation Challenges of IoT-Based Digital Supply Chain (Supply Chain 0/4). arXiv preprint arXiv:2206.12277.