Neutrosophic Sets and Systems, Vol. 55, 2023
University of New Mexico

An Integrated Model for Ranking Risk Management in Industrial Internet of Things (IIoT) system

Abdullah Ali Salamai

Management Department, Applied College, Jazan University, Jazan, KSA

Email: abSalamai@jazanu.edu.sa

Abstract

The Industrial Internet of Things (IIoT) was developed based on the technology and applications of the Internet of Things (IoT) in an industrial environment. As it is a sub-set of the IoT, it requires higher levels of safety and security. While increased productivity, better management and high operational efficiency are its main goals, they involve managing many risks, such as conflicting criteria and uncertain information, that need to be assessed and ranked. Therefore, in this paper, the Multi-criteria Decision-making (MCDM) method is used to deal with these criteria and a neutrosophic environment to overcome the uncertainty. Also, the Analytical Hierarchical Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) approaches are proposed. The former is used to obtain the weights of the criteria and the latter to rank the management of risk in the IIOT system. Numerical examples are provided and a sensitivity analysis conducted to test the reliability of this model.

Keywords: IIoT; IoT; neutrosophic sets; AHP; TOPSIS, risks; SVNSs

1. Introduction

The novelthe IoT that appeared in recent years is based on the development of wireless technologies. In 1998, its concept was introduced by Kevin Ashton for objects or connected to the internet. It has many advantages in applications such as transportation, healthcare and smart homes as well as industry for reducing costs while effectively controlling operations. The concept of the IIoT was introduced based on the innovations and benefits of the IoT in industry. The large amounts of data collected and analyzed by IIoT in industry are used to enhance the performances of industrial systems , provide many services and reduce operational costs [1].

There are several terms for the IIOT, such as Industry 4.0, smart manufacturing and the IoT in industry. The main reason for the IIoT is its use of advanced technologies and applications, including deep learning, machine learning, cloud computing and 5G, for optimizing industrial processes. In 2011, the German government introduced the term Industry 4.0. Its main goal is to collect and analyze the data and information of any product and enhance the efficiency of its manufacture.

The IIoT is a sub-set of the IoT which requires more safety and security. It will enable Industry 5.0 to reduce the gap between humans and machines. By 2025, 70 billion devices will be connected to it and, in 2023, its share in the global market will be USD14.2 trillion.

The IIoT plays a vital role in many fields and companies, such as providers of healthcare, producers of agriculture and manufacturers, to increase their performances, efficiency and productivity through smart management; for example, hospitals can overcome their limitations by using IIoT technologies to connect medical devices. Although the IIoT helps workers to improve efficiency and safety[2], it has many risks which, as they threaten industrial processes and affect the performances of systems, should be ranked in terms of their significance.

The problem of ranking these risks includes uncertainty and vague information. Although a fuzzy set is used to solve the uncertainty, it cannot deal with the value of indeterminacy [3]. To overcome this problem, a neutrosophic set is introduced. It handles both uncertainty and vague information by representing the indeterminacy value.[4] A single-valued neutrosophic set (SVNS) includes the three values of truth, indeterminacy and falsity (T,I,F). It is a sub-set of a neutrosophic set and represents data using single-valued neutrosophic numbers (SVNNs)[5].

As ranking the risks of the IIoT involves different, multiple and conflicting factors, the concept of the Multi-criteria Decision-making (MCDM) method, which solves complex decision-making problems, is used[6]. In this study, the Analytical Hierarchical Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) approaches are employed. The former is used to calculate the weights of the criteria and is a common MCDM method. It depends on a pair-wise comparison of the criteria and alternatives. It helps decision-makers select the best solution and decision given vague and imprecise information. It has been applied to solve medical, engineering, manufacturing and educational problems and is easy to use [7]. In this paper, the TOPSIS method is used to rank the risks in the IIoT. It performs mathematical calculations to compute the best alternatives and is a common MCDM method [8].

The main contributions of this work are as follows.

I. It describes the benefits and risks of the IIoT and ranks these risks to help enterprises, companies, etc. consider them.
II. It uses different units of criteria and alternatives to assess these risks.
III. It employs the MCDM methods AHP and TOPSIS.
IV. It introduces SVNSs to overcome the vagueness and uncertainty of information in the IIoT.

The remainder of this paper is organized as follows: related work is presented in section 2; a hybrid model in section 3; a numerical example in section 4; a sensitivity analysis in section 5; and, finally, conclusions and suggested future work in section 6.

2. Related Work

In this section, a literature review of the IIoT and our model are provided, with the concept of the IIoT and cyber physical systems (CPS) presented in [9, 10]. The IIoT is used in many fields, such as healthcare and agriculture, and many companies. It aids farmers in computing their agricultural variables, such as water and nutrients in the soil as well as the fertilizers used to increase productivity [11, 12]. Many companies, such as Microsoft [13] and the Climate Group encourage agricultural pursuits [14]. Sisinni et al. described the IIoT's challenges, such as energy efficiency, real-time cohabitation and interoperability, privacy and security, as well as its opportunities and directions [2]. . Sadeghi et al. considered privacy and security as its main challenges [15]. They concluded that cyber-attacks are very critical as they cause physical damage and threats to humans. Boyes et al. proposed a framework for analyzing security and sensitivity threats [16]. Younan et al. discussed the IIoT's issues and recommended technologies for them IIoT [17].

As the challenges and risks of the IIoT include a great deal of vague and uncertain information, a fuzzy sets have been used. ElHamdi et al. discussed an agricultural framework using fuzzy sets to compute the best locations for sensors on a shop floor [18]. Collotta et al. used a fuzzy model to enhance power management in smart homes [19]. However, as these sets have several limitations, such as not considering indeterminacy values, neutrosophics ones were used to overcome this uncertainty by taking these values into account. Abdel-Basset et al. used neutrosophic sets to solve the problem of the IoT's transition difficulties [20] which no previous research had considered. Therefore, in this study, SVNSs are proposed to overcome uncertainty of the risks of the IIoT.

As the risks of the IIoT have many different and conflicting criteria and factors, MCDM approaches have been used to overcome this problem [21]. Grida et al. used a MCDM framework to assess the performance of the IoT in a supply chain [22]. Durão et al. used the AHP, which is a common MCDM method for computing the weights of the criteria [23], for the selection process in the IoT [24]. Zhang et al. used the fuzzy AHP method to assess system security in the IoT [25], with another MCDM method, TOPSIS, used to rank the alternatives. Wang and et al. used the fuzzy AHP and TOPSIS methods to design a framework for assessing security in the IoT [26]. Tariq et al. adopted the TOPSIS method to determine the challenges in the medical field using the IoT [27]. Also, Çalık employed it to select green suppliers in the IoT [28].

From the review of the literature, it is clear that no study proposed using SVNSs with the AHP and TOPSIS methods to rank risks in the IIoT.

3. Hybrid Model

In this paper, a hybrid model with SVNSs and MCDM with AHP and TOPSIS methods is proposed. The AHP one is used to calculate the weights of the criteria and the TOPSIS one to rank the risks of the IIoT. The first stage in this hybrid model is using the SVNSs to overcome uncertain information. The research framework is shown in Fig. 1.

3.1. Single-valued Neutrosophic Sets (SVNSs)

A SVNS is a sub-set of a neutrosophic set. It deals with the three values of truth, indeterminancy and falsity (T,I,F). It has the function of scoring accuracy and certainty, and handles vague and inconsistent information well.

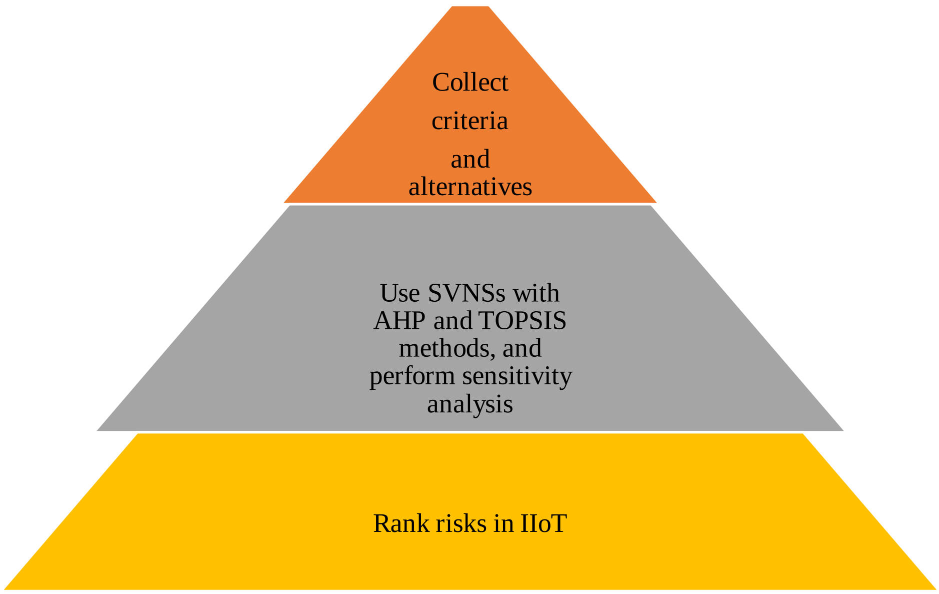

Fig. 1. Research framework

3.2. AHP Method

The AHP method is used to calculate the weights of the criteria. Its steps are illustrated in Fig. 2 and executed as follows [29].

Step 1. Build a pair-wise comparison decision matrix among the criteria using the opinions of experts and decision-makers as

$$A^P = \begin{bmatrix} A_{11}^P & \cdots & A_{1d}^P \\ \vdots & \ddots & \vdots \\ A_{c1}^P & \cdots & A_{cd}^P \end{bmatrix} \quad (1)$$

where P refers to the decision-makers, c the number of criteria and d the number of alternatives.

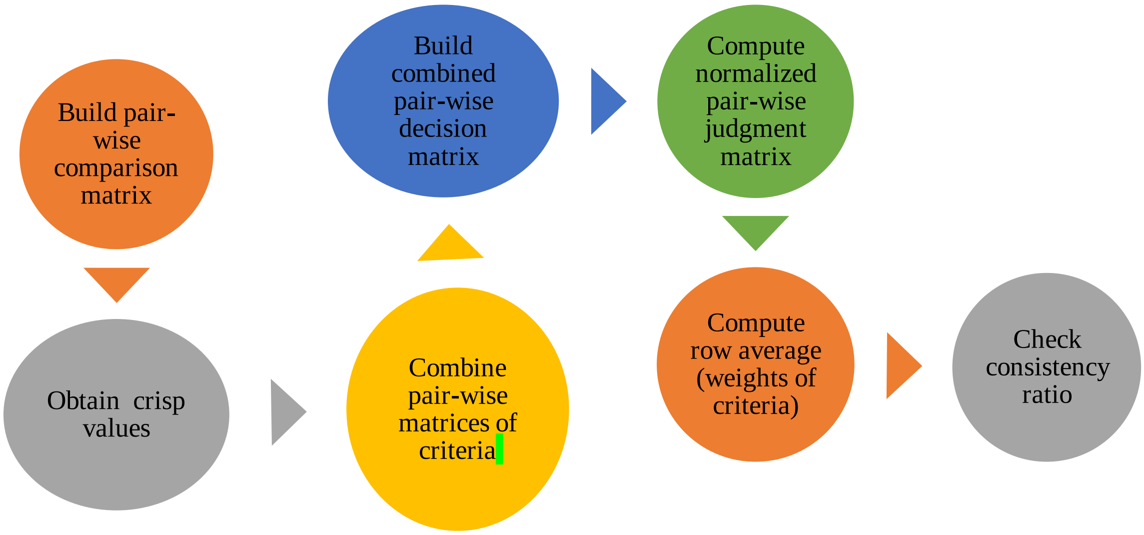

Fig. 2. **S**teps in AHP method

Step 2. Obtain the crisp values by converting the opinions of the decision-makers to SVNNs according to the values in Table 1. Then, convert these numbers to crisp values to obtain one instead of three values using the score function

$$F(A_{rs}^P) = \frac{2 + T_{rs}^P - I_{rs}^P - F_{rs}^P}{3} \quad (2)$$

where T_{rs}^P, I_{rs}^P, F_{rs}^P refer to the truth, indeterminacy and falsity values of the SVNNs' $c = 1,2, \dots r$, $d = 1,2,3, \dots s$.

Table 1. Scales of SVNSs

Linguistic Variable	SVNNs
Very Corrupt	<0.30,0.7,0.75>
Corrupt	<0.40,0.6,0.65>
Equal	<0.6,0.5,0.6>
Honest	<0.85,0.35,0.35>
Very Honest	<0.95,0.2,0.3>

Step 3. Combine the pair-wise matrices of the criteria in one matrix using

$$A_{rs} = \frac{\sum_{P=1}^{P} A_{rs}}{P} \quad (3)$$

Step 4. Build a combined pair-wise decision matrix as

$$\mathrm{A} = \begin{bmatrix} \mathrm{A}_{11} & \cdots & \mathrm{A}_{1s} \\ \vdots & \ddots & \vdots \\ \mathrm{A}_{r1} & \cdots & \mathrm{A}_{rs} \end{bmatrix} \quad (4)$$

Step 5. Compute a normalized pair-wise comparison matrix using the combined pair-wise comparison matrix as

$$\mathrm{Z}_{\mathrm{r}}^{\mathrm{c}} = \frac{\mathrm{A}_{\mathrm{r}}}{\sum_{\mathrm{r}=1}^{\mathrm{c}} \mathrm{A}_{\mathrm{r}}}; \mathrm{r} = 1,2,3, \dots \dots . \mathrm{c} \quad (5)$$

Step 6. Compute the row average (weights of the criteria) after building the normalized pair-wise comparison matrix as

$$\mathrm{w}_{\mathrm{r}} = \frac{\sum_{\mathrm{s}=1}^{\mathrm{d}} (\mathrm{Z}_{\mathrm{rs}})}{\mathrm{s}}; \mathrm{r} = 1,2,3, \dots \dots . \mathrm{c}; \mathrm{s} = 1,2,3, \dots \mathrm{d}; \quad (6)$$

Step 7. Use the consistency ratio

to check the consistency of the opinions of the decision-makers by

$$CR = \frac{CI}{RI} \quad (7)$$

$$CI = \frac{\lambda_{max} - n}{n-1} \quad (8)$$

where RI refers to a random index, CI the consistency index and n the number of criteria.

3.3. TOPSIS Method

This method is used to rank the risks in the IIoT. Its steps are shown in Fig. 3 and described as follows [29].

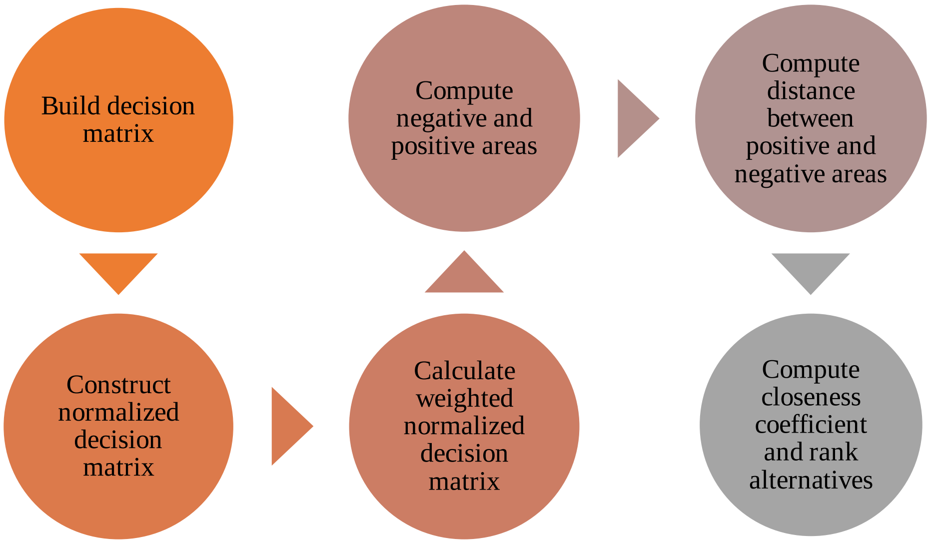

Fig. 3. Steps in TOPSIS method

Step 8. Build a decision matrix of the criteria and alternatives using Eqs. (1), (2), (3) and (4).

Step 9. Construct a normalized decision matrix as

$$Y_{rs} = \frac{A_{rs}}{\sqrt[2]{\sum_{r=1}^{c} A_{rs}^2}} \quad r = 1,2,3, \ldots \ldots, c \text{ and } s = 1,2,3 \ldots \ldots, d \tag{9}$$

Step 10. Calculate the weighted normalized decision matrix by multiplying the normalized decision matrix by the weights of the criteria as

$$X_{rs} = Y_{rs} * W_s \tag{10}$$

Step 11. Compute the negative and positive areas for the positive and negative criteria, respectively, by

$$E_d{}^{+} = \begin{cases} \max(X_{rs}) & for\ positive\ criteria \\ \min(X_{rs}) & for\ negative\ criteria \end{cases} \quad \text{Positive area} \tag{11}$$

$$E_d{}^{-} = \begin{cases} \min(X_{rs}) & for\ positive\ criteria \\ \max(X_{rs}) & for\ negative\ criteria \end{cases} \quad \text{Negative area} \tag{12}$$

Step 12. Calculate the Euclidean distance between the positive and negative areas for the positive and negative criteria, respectively, as

$$I_r^{+} = \sqrt{\sum_{s=1}^{d} (X_{rs} - E_s^{+})^2} \quad \text{for positive criteria} \tag{13}$$

$$I_r^{-} = \sqrt{\sum_{s=1}^{d} (X_{rs} - E_s^{-})^2} \quad \text{for negative criteria} \tag{14}$$

Step 13. Compute the closeness coefficient using Eq. (15) and then rank the alternatives in descending order of H_r as

$$H_r = \frac{I_r^-}{I_r^+ + I_r^-} \tag{15}$$

4. Results obtained from Hybrid Model

The first step in building the hierarchy tree is to determine the goal for this study (ranking the risks in the IIoT) and collect the criteria and alternatives, that is, four main criteria, fourteen sub-criteria and four alternatives, as shown in Fig. 4. The alternatives are A_1 - catastrophic risk, A_2 –cyber-attack risk, A_3 - environmental risk and A_4 - infrastructure Risk, with all the criteria positive.

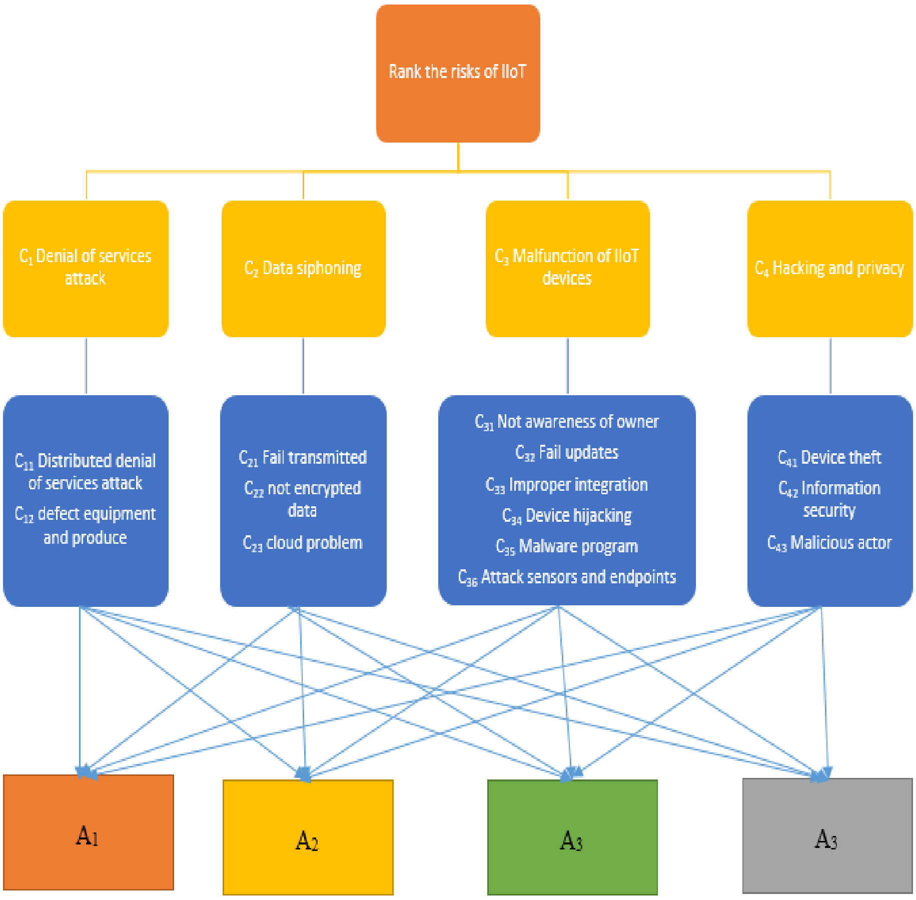

Fig. 4. Goal, criteria and alternatives for this research

Three decision-makers with expertise in the IIoT are proposed. The first has a PhD degree in the IIoT and the others Master's degrees in that field. Beginning with the SVNNs in Table 1, their opinions regarding building the pair-wise comparison matrix using Eq. (1) are obtained. Then, the score function is applied to convert their linguistic terms into values which are converted into three numbers (T,I,F) to obtain one value using Eq. (2). The values of the three pair-wise comparison matrices are then combined in one matrix using Eqs. (3) and(4), and shown in Table 2 for the main criteria and Tables 3.1, 3.2, 3.3, 3.4 for the sub-criteria.

Table 2. Combined pair-wise comparison matrix for main criteria

Criteria	C_1	C_2	C_3	C_4
C_1	0.5	0.49443	0.60557	0.8167
C_2	2.20438	0.5	0.7167	0.75003
C_3	1.79983	1.39528	0.5	0.75003
C_4	1.22444	1.33834	1.33834	0.5

Table 3.1. Combined pair-wise comparison matrix for sub-criteria C_1

Criteria	C_{11}	C_{12}
C_{11}	0.5	0.6389
C_{12}	1.742882	0.5

Table 3.2. Combined pair-wise comparison matrix for sub-criteria C_2

Criteria	C_{21}	C_{22}	C_{23}
C_{21}	0.5	0.527767	0.7167
C_{22}	2.147428	0.5	0.672233
C_{23}	1.395284	1.685934	0.5

Table 3.3. Combined pair-wise comparison matrix for sub-criteria C_3

Criteria	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}	C_{36}
C_{31}	0.5	0.6389	0.6389	0.605567	0.672233	0.605567
C_{32}	1.742882	0.5	0.605567	0.750033	0.6389	0.6389
C_{33}	1.742882	1.79983	0.5	0.672247	0.750033	0.6389
C_{34}	1.79983	1.338336	1.685843	0.5	0.672233	0.750033
C_{35}	1.685934	1.742882	1.338336	1.685934	0.5	0.527767
C_{36}	1.79983	1.742882	1.742882	1.338336	2.147428	0.5

Table 3.4. Combined pair-wise comparison matrix for sub-criteria C_4

Criteria	C_{41}	C_{42}	C_{43}

C_{41}	0.5	0.783367	0.527767
C_{42}	1.281388	0.5	0.6389
C_{43}	2.147428	1.742882	0.5

After building the combined pair-wise comparison matrices, the AHP method is applied to obtain the weights of the criteria. Firstly, Eq. (5) is used to normalize the pair-wise comparison matrix in Table 4 and then the weights of the criteria are computed by Eq. (6). In Table 5. the weights of the main and sub-criteria as well as their local and global weights are shown. The results indicate that the C_4 (hacking and privacy) has the highest weight with a value of 0.2934 and C_1 (denial of service attack) the lowest with a value of 0.1754. In Fig. 5, the weights of the main criteria are illustrated. C_{43} (malicious actor) has the highest weight of the sub-criteria and C_{11} (unaware of owner) the lowest. Then, the consistency ratio is checked to test whether the opinions of the experts are consistent using Eqs. (7) and (8); if it is less than 0.1, they are consistent.

Table 4. Normalized pair-wise comparison matrix for main criteria using AHP method

Criteria	C_1	C_2	C_3	C_4
C_1	0.087281	0.132625	0.191598	0.289942
C_2	0.384799	0.134118	0.226761	0.266275
C_3	0.314181	0.374266	0.158198	0.266275
C_4	0.21374	0.358991	0.423443	0.177508

Table 5. Weights of main and sub-criteria

Criteria	Weights of main criteria	Criteria	Local Weights	Global Weights
C_1	0.175362	C_{11}	0.392	0.068757
		C_{12}	0.608	0.106643
C_2	0.252988	C_{21}	0.233	0.058926
		C_{22}	0.357	0.090285
		C_{23}	0.41	0.103689
C_3	0.27823	C_{31}	0.106	0.0295
		C_{32}	0.129	0.035901
		C_{33}	0.155	0.043137
		C_{34}	0.174	0.048424
		C_{35}	0.192	0.053434
		C_{36}	0.244	0.067905
C_4	0.293421	C_{41}	0.21	0.061614
		C_{42}	0.338	0.099169
		C_{43}	0.452	0.132617

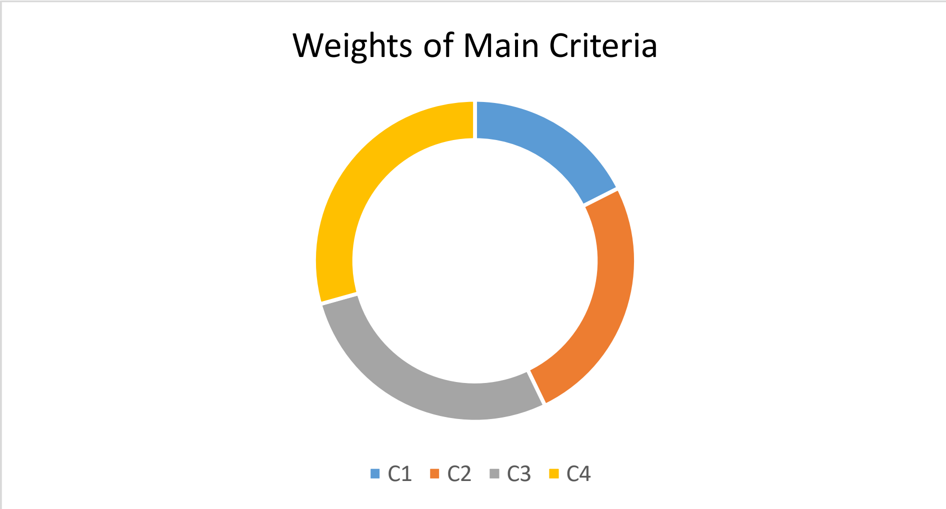

Fig. 5. Weights of main criteria

In applying the TOPSIS method to rank the alternatives, the first step is to build a decision matrix of the criteria and alternatives using Eqs. (1) (2), (3) and (4) (Table 6). Then, the decision matrix is normalized using Eq. (9) (Table 7) and, using Eq. (10), the weighted normalized decision matrix is computed by multiplying the values of the normalized decision matrix by the weights of the criteria (Table 8). As Eqs. (11) and (12) are applied to obtain the positive and negative ideal solutions for the positive and negative criteria, respectively, while all the criteria are positive. The distance from each alternative is computed using Eqs. (13) and (14) for the positive and negative criteria, respectively, and the closeness coefficient using Eq. (15) (Table 9). Finally, the alternatives are ranked in the descending order of the values of the closeness coefficient. Of the risks, the A_2 cyber-attack is the highest and the A_1 catastrophic the lowest. Table 9 shows the ranks of the alternatives and Fig. 6 those of the risks obtained from the TOPSIS method.

Table 6. Combined decision matrixof criteria and alternatives

Criteria\alternatives	C_{11}	C_{12}	C_{21}	C_{22}	C_{23}	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}	C_{36}	C_{41}	C_{42}	C_{43}
A_1	0.67498	0.51665	0.35833	0.67498	0.67498	0.51665	0.67498	0.67498	0.44165	0.35833	0.67498	0.67498	0.35833	0.7583
A_2	0.7958	0.7583	0.48748	0.67498	0.7583	0.51665	0.6458	0.7583	0.35	0.54583	0.7583	0.3875	0.48748	0.599975

A_3	0.56248	0.43333	0.5	0.51665	0.63748	0.71248	0.6833	0.52498	0.40415	0.7583	0.52498	0.7583	0.6458	0.7208
A_4	0.32915	0.7583	0.7958	0.40415	0.7583	0.67498	0.3875	0.44165	0.62915	0.7958	0.51665	0.32915	0.7958	0.433325

Table 7. Normalized decision matrix using TOPSIS method

Criteria\alternatives	C_{11}	C_{12}	C_{21}	C_{22}	C_{23}	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}	C_{36}	C_{41}	C_{42}	C_{43}
A_1	0.548632	0.407845	0.320582	0.582775	0.475854	0.422256	0.553016	0.550883	0.47168	0.280263	0.538151	0.594488	0.301083	0.591715
A_2	0.646841	0.598604	0.436128	0.582775	0.534597	0.422256	0.529113	0.618889	0.373798	0.426916	0.604586	0.341293	0.409602	0.468171
A_3	0.45719	0.342068	0.447334	0.446077	0.449416	0.582303	0.559837	0.42846	0.43163	0.593103	0.418558	0.667877	0.542635	0.562453
A_4	0.267539	0.598604	0.711977	0.348944	0.534597	0.551655	0.317484	0.360454	0.671929	0.622434	0.41192	0.289901	0.668672	0.338131

Table 8. Weighted normalized decision matrix using TOPSIS method

Criteria\alternatives	C_{11}	C_{12}	C_{21}	C_{22}	C_{23}	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}	C_{36}	C_{41}	C_{42}	C_{43}
A_1	0.037722	0.043494	0.018891	0.052616	0.049341	0.012456	0.019854	0.023763	0.022841	0.014975	0.036543	0.036629	0.029858	0.078471
A_2	0.044475	0.063837	0.025699	0.052616	0.055432	0.012456	0.018996	0.026697	0.018101	0.022812	0.041055	0.021028	0.04062	0.062087
A_3	0.031435	0.036479	0.026359	0.040274	0.0466	0.017178	0.020099	0.018482	0.020901	0.031692	0.028422	0.041151	0.053813	0.074590
A_4	0.018395	0.063837	0.041954	0.031505	0.055432	0.016274	0.011398	0.015549	0.032538	0.033259	0.027972	0.017862	0.066312	0.044841

Table 9. Closeness coefficient and ranks of alternatives

Alternative	Closeness Coefficient	Rank
A_1	0.487915	A_2
A_2	0.547426	A_3
A_3	0.541891	A_4
A_4	0.50286	A_1

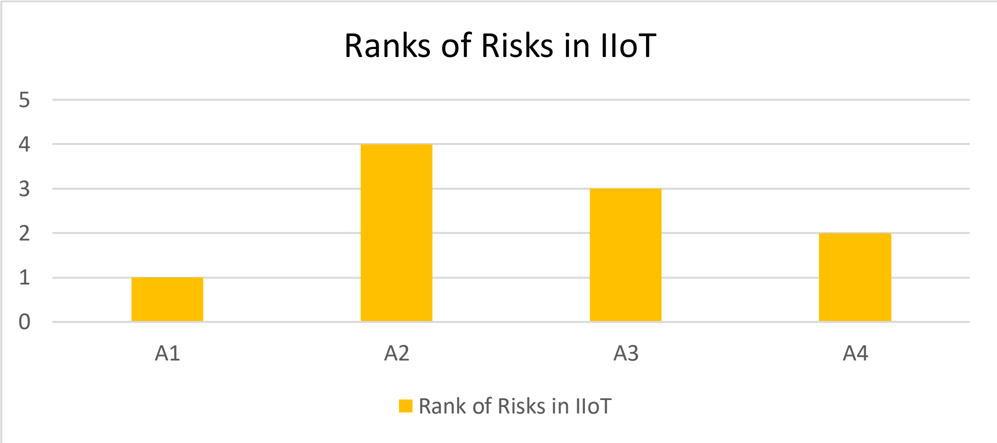

Fig. 6. Ranks of risks in IIoT using TOPSIS method

5. Sensitivity Analysis

When the weights of the criteria change, so do the ranks of the risks. In this sensitivity analysis, five scenarios of changing weights are considered. In the first, all the weights of the criteria are equal and, in the second, that of the first criterion is 0.5 while the others are equal and so on. However, in all the scenarios, the sum of the weights of the criteria must equal 1, as shown in Table 10. When the weights of the main criteria are changed, so are those of the sub-criteria, as shown in Table 11.

Table 10. Five scenarios with different weights of main criteria

Scenario\Criterion	C_1	C_2	C_3	C_4
Scenario 1	0.25	0.25	0.25	0.25
Scenario 2	0.5	0.1667	0.1667	0.1667
Scenario 3	0.1667	0.5	0.1667	0.1667
Scenario 4	0.1667	0.1667	0.5	0.1667
Scenario 5	0.1667	0.1667	0.1667	0.5

Table 11. Sub-criteria for five scenarios with different weights of main criteria

Sub-criterion\weight	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
C_{11}	0.098	0.196	0.065346	0.065346	0.065346
C_{12}	0.152	0.304	0.101354	0.101354	0.101354
C_{21}	0.05825	0.038841	0.1165	0.038841	0.038841
C_{22}	0.08925	0.059512	0.1785	0.059512	0.059512
C_{23}	0.1025	0.068347	0.205	0.068347	0.068347
C_{31}	0.0265	0.01767	0.01767	0.053	0.01767
C_{32}	0.03225	0.021504	0.021504	0.0645	0.021504
C_{33}	0.03875	0.025839	0.025839	0.0775	0.025839
C_{34}	0.0435	0.029006	0.029006	0.087	0.029006
C_{35}	0.048	0.032006	0.032006	0.096	0.032006
C_{36}	0.061	0.040675	0.040675	0.122	0.040675
C_{41}	0.0525	0.035007	0.035007	0.035007	0.105

C_{42}	0.0845	0.056345	0.056345	0.056345	0.169
C_{43}	0.113	0.075348	0.075348	0.075348	0.226

In the next step, the risks are ranked using the TOPSIS method for the different scenarios. In scenarios 1, 2 and 3, A_2 has the highest rank and A_3 the lowest. In scenario 4, A_2 has the highest rank and A_1 the lowest while, in scenario 5, A_3 has the highest rank and A_2 the lowest. The ranks of the risks for the five scenarios are presented in Table 12 and those in the IIoT in Fig. 7.

Table 12. Ranks of risks for five scenarios

Alternative	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
A_1	A_2	A_2	A_2	A_2	A_3
A_2	A_4	A_4	A_4	A_4	A_1
A_3	A_1	A_1	A_1	A_3	A_4
A_4	A_3	A_3	A_3	A_1	A_2

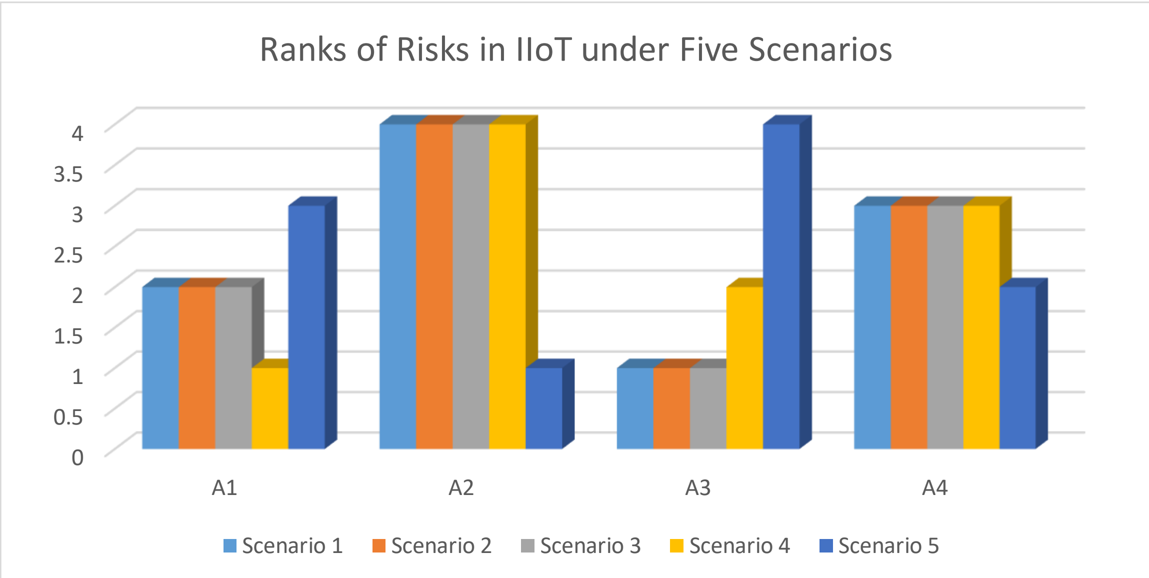

Fig. 7. Ranks of risks in IIoT for five scenarios

6. Conclusions

In this research, SVNSs using MCDM methods rank the risks in the IIoT and the importance of the role the IIoT plays in increasing a system's productivity, efficiency and performance by using the proposed hybrid model. This model includes the AHP and TOPSIS methods, with the former ranking the weights of the criteria and the latter the weights of the criteria. The neutrosophic environment overcomes the vague and uncertain information by considering the indeterminacy value. Four main criteria, fourteen sub-criteria, four alternatives and three decision-makers are adopted in this study.

Future work on this topic will apply other MCDM methods, such as VIKOR, to build a fuzzy model and compare it with the neutrosophic one.

References

1. Khan, W.Z., et al., *Industrial internet of things: Recent advances, enabling technologies and open challenges.* Computers & Electrical Engineering, 2020. **81**: p. 106522.
2. Sisinni, E., et al., *Industrial internet of things: Challenges, opportunities, and directions.* IEEE Transactions on Industrial Informatics, 2018. **14**(11): p. 4724-4734.
3. Abdel-Basset, M., et al., *Three-way decisions based on neutrosophic sets and AHP-QFD framework for supplier selection problem.* Future Generation Computer Systems, 2018. **89**: p. 19-30.
4. Abdel-Baset, M., V. Chang, and A. Gamal, *Evaluation of the green supply chain management practices: A novel neutrosophic approach.* Computers in Industry, 2019. **108**: p. 210-220.
5. Tian, Z.-P., J.-Q. Wang, and H.-Y. Zhang, *Hybrid single-valued neutrosophic MCGDM with QFD for market segment evaluation and selection.* Journal of Intelligent & Fuzzy Systems, 2018. **34**(1): p. 177-187.
6. Tsaur, S.-H., T.-Y. Chang, and C.-H. Yen, *The evaluation of airline service quality by fuzzy MCDM.* Tourism management, 2002. **23**(2): p. 107-115.
7. Lyu, H.-M., et al., *Inundation risk assessment of metro system using AHP and TFN-AHP in Shenzhen.* Sustainable Cities and Society, 2020. **56**: p. 102103.
8. Anser, M.K., et al., *Assessing the integration of solar power projects: SWOT-based AHP–F-TOPSIS case study of Turkey.* Environmental Science and Pollution Research, 2020. **27**(25): p. 31737-31749.
9. Gershenfeld, N.A. and N. Gershenfeld, *When things start to think.* 2000: Macmillan.
10. Radanliev, P., et al., *Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains.* Cybersecurity, 2020. **3**: p. 1-21.
11. Kim, H.-J., K.A. Sudduth, and J.W. Hummel, *Soil macronutrient sensing for precision agriculture.* Journal of Environmental Monitoring, 2009. **11**(10): p. 1810-1824.
12. Mueller, N.D., et al., *Closing yield gaps through nutrient and water management.* Nature, 2012. **490**(7419): p. 254-257.
13. Vasisht, D., et al. *Farmbeats: An iot platform for data-driven agriculture.* in *14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17)*. 2017.
14. Abd El-Mawla, N., M. Badawy, and H. Arafat, *IoT for the failure of climate-change mitigation and adaptation and IIoT as a future solution.* World J. Environ. Eng., 2019. **6**(1): p. 7-16.
15. Sadeghi, A.-R., C. Wachsmann, and M. Waidner. *Security and privacy challenges in industrial internet of things.* in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. 2015. IEEE.
16. Boyes, H., et al., *The industrial internet of things (IIoT): An analysis framework.* Computers in industry, 2018. **101**: p. 1-12.
17. Younan, M., et al., *Challenges and recommended technologies for the industrial internet of things: A comprehensive review.* Measurement, 2020. **151**: p. 107198.
18. El Hamdi, S., et al., *Fuzzy Approach for Locating Sensors in Industrial Internet of Things.* Procedia computer science, 2019. **160**: p. 772-777.

19. Collotta, M. and G. Pau, *Bluetooth for Internet of Things: A fuzzy approach to improve power management in smart homes.* Computers & Electrical Engineering, 2015. **44**: p. 137-152.
20. Abdel-Basset, M., et al., *Utilising neutrosophic theory to solve transition difficulties of IoT-based enterprises.* Enterprise Information Systems, 2020. **14**(9-10): p. 1304-1324.
21. Nada A. Nabeeh , Alshaimaa A. Tantawy, A Neutrosophic Model for Blockchain Platform Selection based on SWARA and WSM, Neutrosophic and Information Fusion, Vol. 1 , No. 2 , (2023) : 29-43 (Doi : https://doi.org/10.54216/NIF.010204).
22. Grida, M., R. Mohamed, and A.N.H. Zaied, *A Novel Plithogenic MCDM Framework for Evaluating the Performance of IoT Based Supply Chain.* Neutrosophic Sets and Systems, 2020. **33**(1): p. 323-341.
23. Ly, P.T.M., et al., *Fuzzy AHP analysis of Internet of Things (IoT) in enterprises.* Technological Forecasting and Social Change, 2018. **136**: p. 1-13.
24. Durão, L.F.C., et al., *Internet of Things process selection: AHP selection method.* The International Journal of Advanced Manufacturing Technology, 2018. **99**(9): p. 2623-2634.
25. Ahmed M. Ali, Ranking Renewable Energy Alternatives by using Triangular Neutrosophic Sets Integrated with MCDM, Neutrosophic and Information Fusion, Vol. 1 , No. 1 , (2023) : 17-26 (Doi : https://doi.org/10.54216/NIF.010102).
26. Wang, L., et al., *ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods.* IEEE Access, 2020. **8**: p. 152316-152332.
27. Tariq, M.I., et al., *Evaluation of the Challenges in the Internet of Medical Things with Multicriteria Decision Making (AHP and TOPSIS) to Overcome Its Obstruction under Fuzzy Environment.* Mobile Information Systems, 2020. **2020**.
28. Çalık, A., *A novel Pythagorean fuzzy AHP and fuzzy TOPSIS methodology for green supplier selection in the Industry 4.0 era.* Soft Computing, 2021. **25**(3): p. 2253-2265.
29. Mona Mohamed , Nissreen El Saber, Prioritization Thermochemical Materials based on Neutrosophic sets Hybrid MULTIMOORA Ranker Method, Neutrosophic and Information Fusion, Vol. 2 , No. 1 , (2023) : 08-22 (Doi : https://doi.org/10.54216/NIF.020101)

Received: August 01, 2022. Accepted: January 04, 2023