Artificial Intelligence in Cybersecurity

Journal Homepage: sciencesforce.com/aics

Artificial Intell. Cyb. Vol. 1 (2024) 21–36

Paper Type: Original Article

Assessment of Cybersecurity in Industry 4.0 using Delphi-Based Factor Relationships and Comprehensive Distance-Based Ranking Methods under Uncertainty

Mai Mohamed [1,*], Shaimaa Ayman [1] and Jun Ye [2]

[1] Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Sharqiyah, Egypt; Emails: mmgaafar@zu.edu.eg; sh.ayman021@fci.zu.edu.eg.

[2] School of Civil and Environmental Engineering, Ningbo University, Ningbo, Zhejiang, China; yejun1@nbu.edu.cn.

Received: 27 Feb 2024 **Revised**: 13 May 2024 **Accepted**: 11 Jun 2024 **Published**: 14 Jun 2024

Abstract

Industry 4.0 is a new revolution in which internet connection technologies are interfaced with various components of industrial systems to create the smart factories and manufacturing organizations of the future to achieve a sustainable manufacturing framework. A large number of networked devices presents a significant chance to gather important data for improving the technology of decision-making to enhance product life-cycle management. Industry 4.0 technologies will face significant challenges and obstacles due to the cybersecurity and data privacy problems suffered by current Internet technology. In actuality, cybersecurity poses an important challenge to the advancement of sustainable manufacturing. Cybersecurity architectures are widely employed to prevent intrusions and attacks on computers and networks. As a result, there is a major decrease in the adoption of Industry 4.0 technologies and the sustainable manufacturing framework within organizations. To achieve the implementation of this sustainable manufacturing in companies we suggested five cybersecurity measures and six criteria. The proposed decision-making method aims to rank the cybersecurity procedures. The ranking of these measures used a combination of Delphi-FARE (factor relationship) and COBRA (comprehensive distance-based ranking) methods based on a neutrosophic environment. The result showed that alternative one "Data Encryptions" is the best one, and alternative five "Cloud Servers" is the worst one. We conducted a sensitivity and comparison analysis to verify the stability of the model and its performance with other models and demonstrated impressive results.

Keywords: Industry 4.0; Cybersecurity; Uncertainty; Data Encryption, Sustainable Manufacturing.

1 | Introduction

Industry 4.0, often known as the fourth industrial revolution, is characterized by patents and until now unheard-of amounts of data sharing. It is a revolutionary development whereby internet connection technologies are interfaced with various components of industrial systems to create smart factories and manufacturing companies. The phrase "industry 4.0," was first introduced in a high-technology strategy project in 2011 [1]. Reaching new heights in Industry 4.0 through the togetherness of computer networks and real-life physical processes through the use of cutting-edge technologies such as cloud computing

Corresponding Author: mmgaafar@zu.edu.eg

https://doi.org/10.61356/j.aics.2024.1296

Licensee **Artificial Intelligence in Cybersecurity**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

technologies, augmented reality (AR), cyber-physical IoT systems, blockchain, and increasingly smarter robotics applications that are part of the hyper-connectedness of Industry 4.0 [2]. The Industry Internet of Things (IIoT) is a component of the IT generation, which is dependent on modern cloud systems and web technology. The data generated by IoTs is subjected to big data analytics, machine learning, and other AI models, which are vulnerable to data inference attacks [3]. The previously mentioned technologies already existed to some extent before the beginning of Industry 4.0. Some authors have questioned whether Industry 4.0 technology represents an evolution or a revolution, as it has allowed the integration of previously developed applications, technologies, and solutions, and can be considered a new social, political, and economic concept [4].

The digital business process among smart industrial organizations, however, raises worries among stakeholders for production businesses' management on the security of their databases, which contain information on orders, contractors, and all things about production. Companies and manufacturers are well aware of the potential consequences and damage caused by cyber-attacks. The effects can be damaging to customer trust and brand reputation. In industrial environments, an attack could result in millions of dollars in downtime and disruption to production plans. Therefore, in order to guarantee that Industry 4.0 is widely used, cybersecurity must be adopted. There are two categories of cybersecurity threats: internal and external. The growing number of internal threats, such as employees' intentional or unintentional disclosure of confidential information, pose a threat to an organization's IT security. The most difficult component of protecting against external threats is adapting to more advanced and frequent attacking techniques. It takes IT security skills for a manufacturing organization not to install a reliable antivirus application on an organization's computers [5].

Among a lot of advantages, Industry 4.0 can provide manufacturing companies with successful business models, increased productivity, quality, and better working environments [6]. However, disadvantages like ignorance, lack of awareness, expenses, and possible energy drawbacks have complicated assessment decisions for example that discusses blockchain technology problems [7]. These Industry 4.0 technologies are new among small and medium-sized businesses and emerging nations. More complete comprehension and advancements are necessary for broader acceptance. This includes the impact of Industry 4.0 on sustainability. For social sustainability, intelligent and autonomous production systems can enhance worker health and safety while also increasing worker motivation and satisfaction. [8]. One major obstacle impeding the adoption of sustainable development concepts in businesses and manufacturing processes is the implementation of cybersecurity measures.

Some researchers defined the phrase Industry 4. as the implementation of novel ideas and technology in the value chain's structure [6], some defined it as the intricate solution developed in the areas of engineering, computer science, and management [9], and others, defined as the industry's intelligent networking of devices and measures through the use of information and communication technology [10]. Several researchers presented many measurements for sustainable manufacturing in Industry 4.0 such as the Industrial Internet of Things (IIOT) [11], Optimization and Simulation [12], Big Data Analysis [13], Autonomous robots [14], Cloud Computing [15], Additive Manufacturing, and Cybersecurity [16]. A new industrial paradigm has resulted in new logistical requirements. According to Jeschke [17], logistics 4.0 is an integral part of industry 4.0, which is the application of different industry 4.0 technologies in logistics. also, studies have been conducted on the application assessment of Industry 4.0 technologies across a range of domains, including logistics [18]. Dominique et al. [19] presented a study suggesting that after the spread of COVID-19, stakeholder collaboration will be essential and that the adoption of digital technologies will promote sustainable manufacturing for Industry 4.0. Torbacki [20] suggested a framework in the area of cybersecurity utilized by organizations for sustainable manufacturing and sustainable Industry 4.0 using DANP and PROMETHEE II. According to Bhosale et al. [21], the main threat-agent categories for connected and autonomous vehicles have been determined from the body of research and cybersecurity studies. Marion et al. [22] developed a framework that provides a strong base that can be customized to meet our needs for

addressing the danger of data manipulation, evaluating cybersecurity frameworks, and determining which choice is the most flexible.

Particularly in the last decade, the MCDM study field has expanded rapidly. However, a broader application is dependent on their ability to address a specific issue and the quantity of resources (human, logistical, financial, etc.) required for their implementation. There is no right or wrong approach, just approaches that are more or less appropriate for the task and the available resources. In this study, we are analyzing the measures for cybersecurity in Industry 4.0 for achieving sustainable manufacturing. This research aims to develop a novel methodology based on IVNS-Delphi-FARE including factor relationship and comprehensive distance-based ranking (COBRA) methods.

The remainder sections of this paper are organized as follows: A basic concept of interval-valued neutrosophic sets is given in Section 2. Section 3 explains the Delphi method. Section 4 offers the FARE method. The framework of cybersecurity in Industry 4.0, measures are ranked in Section 5 using D-FARE COBRA based on IVNS. Section 6 gives a sensitivity analysis. Section 7 presents a comparative analysis. Section 8 presents the conclusion.

2 | Interval-Valued Neutrosophic Sets (IVNS)

In this section, we present some concepts of interval-valued neutrosophic sets [23], which we will need in this study.

Definition 2.1. Supposing X be a space of objects with generic elements X denoted by x. An interval-valued neutrosophic set numbers (IVNNs) A is expressed, where$T_A(x) = [T_A^L, T_A^U]$ is an interval truth-membership function, $I_A(x) = [I_A^L, I_A^U]$ is an interval indeterminacy-membership function, $F_A(x) = [F_A^L, F_A^U]$ is an interval falsity-membership function, by

$$A = <[\mathrm{T}_\mathrm{A}^\mathrm{L}, \mathrm{T}_\mathrm{A}^\mathrm{U}], [\mathrm{I}^\mathrm{L}, \mathrm{I}^\mathrm{U}], [\mathrm{F}^\mathrm{L}, \mathrm{F}^\mathrm{U}]> \tag{1}$$

For each $x \in X$, where $T_A(x), I_A(x), F_A(x) \subseteq [0,1]$, and also execute the condition $0 \leq Sup\, T_A(x) + SupI_A(x) + SupF_A(x) \leq 3$.

Definition 2.2. Determining the IVNS evaluation scale to obtain experts' opinions as shown in Table 1.

Table 1. The interval-valued neutrosophic numbers set IVNNs scale [24].

Linguistic term	Neutrosophic sets
Equal importance	$< [0.5, 0.5], [0.5, 0.5], [0.5, 0.5] >$
Weakly more importance	<[0.50, 0.60], [0.35, 0.45], [0.40, 0.50]>
Moderate importance	$< [0.55, 0.65], [0.30, 0.40], [0.35, 0.45] >$
Moderately more importance	$< [0.60, 0.70], [0.25, 0.35], [0.30, 0.40] >$
Strong importance	$< [0.65, 0.75], [0.20, 0.30], [0.25, 0.35] >$
Strongly more importance	$< [0.70, 0.80], [0.15, 0.25], [0.20, 0.30] >$
Very strong importance	$< [0.75, 0.85], [0.10, 0.20], [0.15, 0.25] >$
Very strongly importance	$< [0.80, 0.90], [0.05, 0.10], [0.10, 0.20] >$
Extreme importance	$< [0.90, 0.95], [0, 0.05], [0.05, 0.15] >$
Extremely high importance	$< [0.95, 1.0], [0.0, 0.0], [0.0, 0.10] >$
Absolutely more importance	$< [1.0, 1.0], [0.0, 0.0], [0.0, 0.0] >$

Definition 2.3. Determining the score functions $S(x)$ of IVNNs by Eq. (2).

$$\mathrm{S(x)} = \left(\frac{1}{4}\right) \times \left[2 + \mathrm{T}_\mathrm{A}^\mathrm{L} + \mathrm{T}_\mathrm{A}^\mathrm{U} - \left(2\mathrm{I}_\mathrm{A}^\mathrm{L}\right) - \left(2\mathrm{I}_\mathrm{A}^\mathrm{U}\right) - \mathrm{F}_\mathrm{A}^\mathrm{L} - \mathrm{F}_\mathrm{A}^\mathrm{U}\right] \tag{2}$$

Definition 2.4. Aggregate the crisp value by using the average in Eq. (3).

$$X_U = \frac{[T_A^L(x), T_A^U(x)], [I_A^L(x), I_A^U(x)], [F_A^L, F_A^U]}{n} \quad (3)$$

Where n number of experts.

3 | The FARE Method

The FARE (Factor Relationship) model was proposed by Ginevi˘cius [25] to calculate the criterion weights in the MCDM approach based on the relationships among all the criteria. The experts are asked to provide the amount of preliminary information. The relationships between the other criteria in the set and their direction are then analytically defined by the first stage's established criteria. The criteria weights can be determined once the overall impact of every individual criterion on the other criteria in the set. It is predicated on drawing lines connecting the criteria of the decision-making process as in Figure 1 [26]. The quantitative evaluation scale [27] which is presented in Table 2 used for ranking criteria and assessment of their inter-relationship between system criteria.

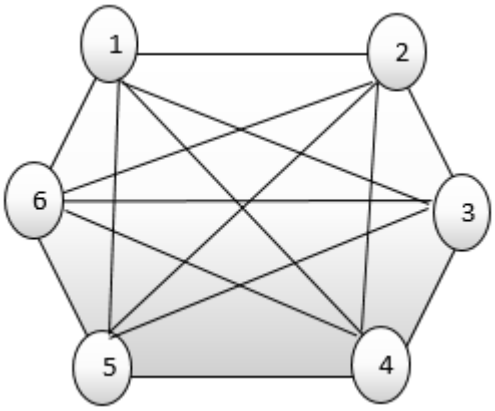

Figure 1. The relationships between the criteria.

Table 2. The scale of quantitative evaluation of the interrelationship between the system's [27].

Type of the effect Produced	Rating of the effect produced by interrelationship (in points)	Corresponding negative Ratings
Almost none	1	−1
Very weak	2	−2
Weak	3	−3
Average	4	−4
Higher than average	5	−5
Strong	6	−6
Very strong	7	−7
Almost absolute	8	−8
Absolute	9	−9

Definition 3.1. Determining the potential impact of the criteria according to the experts as follows:

$$p_j = s_j(n-1) \quad (4)$$

Where $p_j\ x,$ is the potential impact of the criteria, n number of criteria, s_j is the maximum value of the evaluation scale.

Definition 3.2. Determining the impact of criteria on major criteria in which part of the potential impact of the criteria has been transferred to the first criteria as Eq. (5).

$$a_{1j} = a - a_{1l} \quad (5)$$

where a_{1j} is the impact of the jth criterion on the first main criterion C1 and a_{1l} is the part of the jth criterion potential impact transmitted to the C1.

Definition 3.3. Determining the total potential impact of all criteria is calculated using Eq. (6).

$$p_j = \sum_{j=1}^{n} a_{1j} \tag{6}$$

Definition 3.4: Computing the factual potential impact of the jth criterion by Eq. (7).

$$p_j^f = p_j + p = p_j + s_j(n-1) \tag{7}$$

Definition 3.5. Computing the criteria weights by Eq. (8).

$$w_j = \frac{p_j^f}{p_s} = \frac{p_1 - na_{1j} + s_j(n-1)}{ns_j(n-1)} \tag{8}$$

4 | The Delphi Method

A team of academics (Dalkey and Heimer) at the Research and Development (RAND) Corporation, a nonprofit corporation founded for the public welfare and security of the United States, created the Delphi technique [28]. Originally intended as an interactive, methodical forecasting technique based on a panel of experts, to develop the structured qualitative group communication method. This technique has been used to evaluate renewable energy development projects [29] and has other wide applications in several fields in industrial and energy systems in traditional forms, by itself or in merger with other methodologies [30]. This approach was developed and used for a systematic study that needed to get the most trustworthy opinion consensus from specialists. These experts were given a series of questionnaires to complete and then received controlled feedback to reach an agreement. So, the Delphi technique is an interactive process that relies on a questionnaire and surveys based on the answers provided by experts in multiple rounds. For every round, an anonymous synopsis of the experts' opinions is presented. These iterative questionnaires keep going until they reach a consensus and integrate expert opinions. It was used to determine the values of criteria weights, which were supposed to be equal and were used to create the ranking. After alternative evaluations produced decision matrices, contradiction analyses were performed, and the resulting contradiction rates were displayed. We need to determine the degree of the most important criterion. For this reason, this questionnaire was created to enable comparisons between criteria. The cybersecurity measures in the Industry 4.0 questionnaire highlight the purpose of the research, which determines the importance of the criteria. The Delphi technique has been used recently, either by itself or in conjunction with other methods and we will use FARE with it.

5 | The COBRA Method

In this section, we presented the Comprehensive Distance Based Ranking (COBRA) method which was proposed by [10], and used a unique method to rank alternatives according to how far away they are from three different types of solutions: average, negative ideal, and positive ideal.

Definition 5.1. Forming the decision matrix x by determining the assessments (x_{ij}) of the options $(i = 1, \ldots, n)$ in respect to the criteria $(j = 1, \ldots, m)$.

$$x = \left[\begin{pmatrix} x_{11} & \cdots & x_{1m} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nm} \end{pmatrix}\right] \tag{9}$$

where n is the total number of criteria, and m is the total number of the alternatives.

Definition 5.2. Forming the normalized decision matrix by Eq. (10).

$$\delta_{ij} = \frac{x_{ij}}{\max x_{ij}} \tag{10}$$

Definition 5.3. Forming the weighted normalized decision matrix by Eq. (11).

$$A = [w_j \times \delta_{ij}]_{n\times m} \tag{11}$$

Definition 5.4. Determining the positive ideal PIS_j, the negative ideal NIS_j and the average solution AS_j for each criterion by following equations.

$$PIS_j = max(w_j \times \delta_{ij}) \quad \forall\, j \in \text{ Benefit} \tag{12}$$

$$PIS_j = min(w_j \times \delta_{ij}) \quad \forall\, j \in \text{ Cost} \tag{13}$$

$$NIS_j = min(w_j \times \delta_{ij}) \quad \forall\, j \in \text{ Benefit} \tag{15}$$

$$NIS_j = max(w_j \times \delta_{ij}) \quad \forall\, j \in \text{ Cost} \tag{16}$$

$$AS_j = \frac{\sum_{i=1}^{n}(w_j \times \delta_{ij})}{n} \quad \forall\, j \in \text{ Benefit, Cost} \tag{17}$$

Definition 5.5. Calculating the Euclidian dE and Taxicab dT distances for the positive ideal solution.

$$dE(PIS_j)_i = \sqrt{\sum_{j=1}^{m}(PIS_j - w_j \times \delta_{ij})^2} \tag{18}$$

$$dT(PIS_j)_i = \sum_{j=1}^{m}\left|(PIS_j - w_j \times \delta_{ij})\right| \tag{19}$$

For the negative ideal solution:

$$dE(NIS_j)_i = \sqrt{\sum_{j=1}^{m}(NIS_j - w_j \times \delta_{ij})^2} \tag{20}$$

$$dT(NIS_j)_i = \sum_{j=1}^{m}\left|(NIS_j - w_j \times \delta_{ij})\right| \tag{21}$$

For the positive distance of the average solution:

$$dE(AS_j)_i{}^{+} = \sqrt{\sum_{j=1}^{m}\tau^{+}(AS_j - w_j \times \delta_{ij})^2} \tag{22}$$

$$dT(AS_j)_i{}^{+} = \sum_{j=1}^{m}\tau^{+}\left|(AS_j - w_j \times \delta_{ij})\right| \tag{23}$$

$$\tau^{+} = \begin{cases} 1 & if\ AS_j < w_j \times \delta_{ij} \\ 0 & if\ AS_j > w_j \times \delta_{ij} \end{cases} \tag{24}$$

For the negative distance of the average solution:

$$dE(AS_j)_i{}^{-} = \sqrt{\sum_{j=1}^{m}\tau^{-}(AS_j - w_j \times \delta_{ij})^2} \tag{25}$$

$$dT(AS_j)_i{}^{-} = \sum_{j=1}^{m}\tau^{-}\left|(AS_j - w_j \times \delta_{ij})\right| \tag{26}$$

$$\tau^{-} = \begin{cases} 1 & if\ AS_j > w_j \times \delta_{ij} \\ 0 & if\ AS_j < w_j \times \delta_{ij} \end{cases} \tag{27}$$

Definition 5.6. Determining the distances of the positive ideal solutions and the distances of negative ideal solutions, the positive distances of the average solution, and the negative distances of the average solution for each alternative by following Eq. (28).

$$d(S_j) = dE(S_j) + \sigma \times dE(S_j) \times dT(S_j) \tag{28}$$

Where S_j is the solution of (PIS_j, NIS_j, AS_j), σ is the correction coefficient obtained by Eq. (29).

$$\sigma = max\ dE(S_j) - \min dE(S_j) \tag{29}$$

Definition 5.7. Ranking the alternatives based on the increasing values of the comprehensive distances dC_i by Eq. (30).

$$dC_i = \frac{d(PIS_j)_i - d(NIS_j)_i - d(AS_j)_i^{+} + d(AS_j)_i^{-}}{4} \tag{30}$$

6 | Case Study: Assessment of Cybersecurity Measures in Industry 4.0 using Proposed IVN-D-FARE-COBRA Method

The proposed approach suggests a hybrid approach to decision-making, which is a combination of IVNS -D-FARE (Interval-Valued Neutrosophic Numbers Set– Delphi – Factor Relationship methods) [25], [23], [28] and Comprehensive Distance Based Ranking (COBRA) method [10] to prioritize cybersecurity measures or procedures in Industry 4.0. This research has six criteria which are Awareness and Training C1, Waste of Materials and Energy C2, Software Affordable C3, Improvement Procedures C4, Operating Downtime C5, and Cyber Attack C6, for evaluating five cybersecurity measures, these measures are Data Encryptions A1, Network Security A2, Regular Audits and Monitoring A3, Software Versions A4, Cloud Servers A5. As shown in Table 3 many criteria must be taken to evaluate the proposed model.

Table 3. The Criteria of cybersecurity measures in Industry 4.0 for sustainability manufacture.

Criteria	Descriptions
Awareness and Training C1	Increase awareness among Industry 4.0 actors and train them to deal with any threat
Waste of Materials and Energy C2	As a result of data falsification that occurs among participants in Industry 4.0
Software Affordable C3	The fee that you pay to get the software should be more affordable
Improvement Procedures C4	Improve technical measures to ensure Industry 4.0 security
Operating Downtime C5	The amount of time that a device is unavailable, and can be caused by hardware or software, maintenance, upgrades, power outages, network issues, and human error
Cyber Attack C6	Secure the industry supply chain management operations to repel an attack

Also, the set of alternatives of cybersecurity measures in Industry 4.0 to sustainability manufacture is needed for the evaluation as in Table 4.

Table 4: alternatives of cybersecurity measures in Industry 4.0 to sustainability manufacture.

Alternatives	Descriptions
Data Encryptions A1	Modifying data is regarded as a major risk to organizations, with disastrous outcomes. Organizations must implement a cybersecurity framework to defend themselves from these online dangers
Network Security A2	A structure for network data and servers that keeps an organization's network secure and monitors and responds to attack threats
Regular Audits and Monitoring A3	Organizations may regularly check and monitor business processes for compliance with any deviation from the deliberate levels of effectiveness and performance, thanks to continuous monitoring
Software Versions A4	Organizations should always look for updated and upgraded software versions to get the best results, performance, and efficiency
Cloud Servers A5	An important pillar of Industry 4.0 technology for smart factories and smart production that enables easier, more intuitive, and cost-effective systems

The comparison matrices were established based on evaluations of the previous five alternatives regarding six criteria. The Delphi method was used to obtain more accurate results based on a panel of experts' consensus and the FARE (Factor Relationship) method was used to determine the weights of criteria for each cybersecurity measure in Industry 4.0. It eliminates the contradictions that existed in the comparison matrixes, weights could then be computed and contradictions eliminated.

To determine the most effective cybersecurity measures in Industry 4.0 propose solutions to get over impediments, and apply neutrosophic COBRA to rank the alternatives, experts were given the assignment to determine the important criteria that received the highest ranking in multiple rounds. In the first round, stakeholders submitted research topics, and experts grouped them according to themes. In the second round, stakeholders ranked all research questions based on their responses to a survey. In the final round, stakeholders worked on research proposals after evaluating questions with the highest scores and grouped them. We used the quantitative evaluation scale in Table 2 for the interrelationships between system criteria. The goal of this ranking is for the lower-order criterion to have less impact on the higher-order criteria. This means that higher criteria weights should be assigned to higher rating criteria. Figure 2, describes the steps to implement the proposed model for the process of integrating the multi-criteria decision-making MCDM approach of FARE (Factor Relationship) and the Delphi which is based on the relationships between all the criteria for the definition of criteria weights.

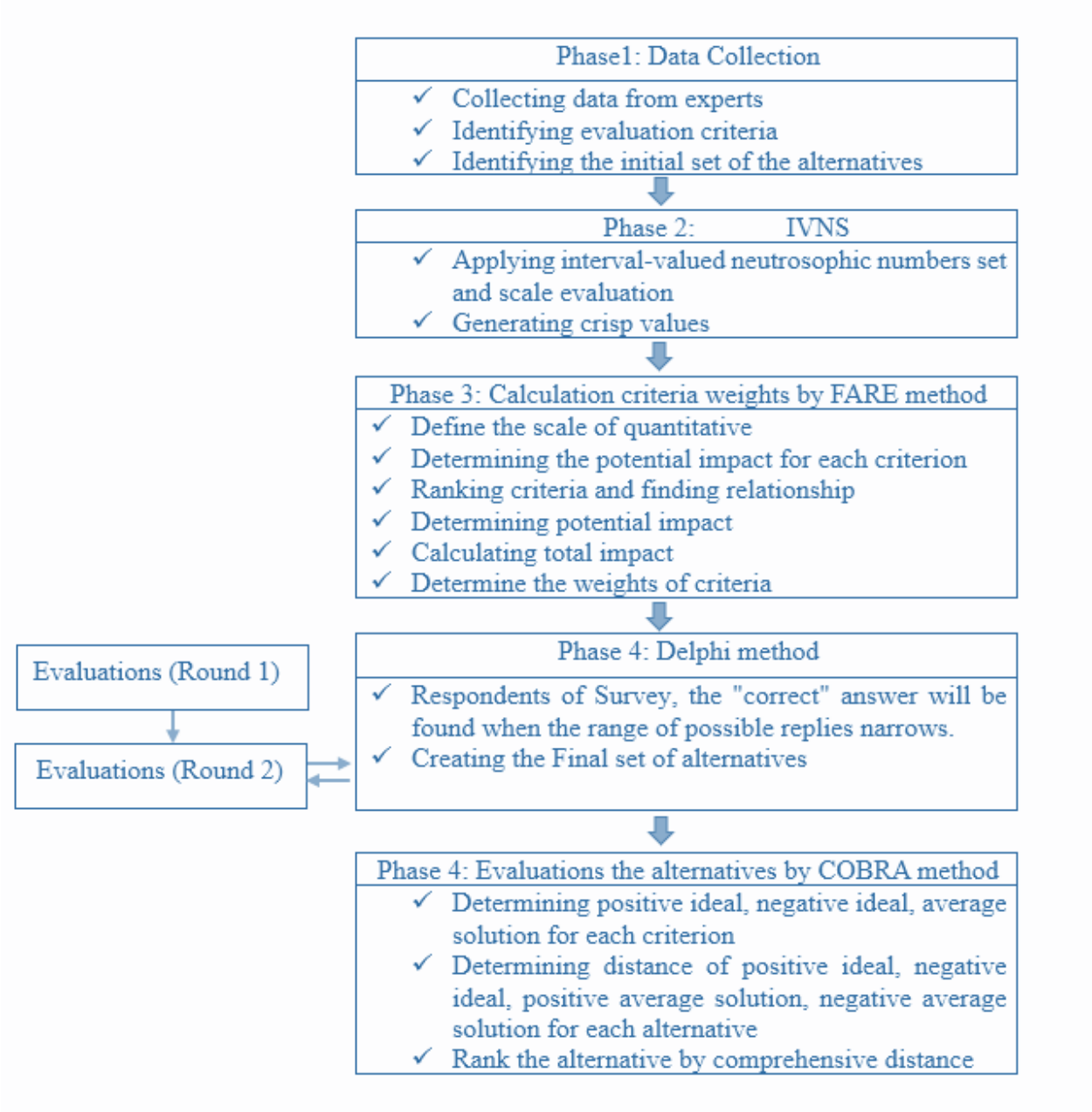

Figure 2. The conceptual proposed framework of the MCDM model.

Step 1. Establish the decision matrix.

The goal is to order the cybersecurity measures in Industry 4.0 to sustainability manufacturers. Suppose that the selected set of criteria is $C = (C1, C2, C3, C4, C5, C6)$, set of cybersecurity measures are $A = (A1, A2, A3, A4, A5)$, and Ex = (Ex_1, Ex_2, Ex_3) be a set of experts.

Step 2. Construct the models and the decision matrix by converting linguistic variables into Interval-Valued Neutrosophic Numbers using Table 1, and aggregate the decision matrix by using Eq. (3) as displayed in Table 5.

Table 5. The aggregated matrix of the expert's opinions.

	C1	C2	C3	C4	C5	C6
A1	<[0.683,0.733], [0.25,0.283], [0.267,0.333]>	<[0.65,0.75], [0.2,0.3], [0.25,0.35]>	<[0.75,0.817], [0.15,0.217], [0.183,0.25]>	<[0.617,0.717], [0.233,0.333], [0.283,0.383]>	<[0.817,0.883], [0.067,0.133], [0.117,0.217]>	<[0.65,0.7], [0.283,0.317], [0.3,0.367]>
A2	<[0.7,0.767], [0.2,0.267], [0.233,0.3]>	<[0.75,0.817], [0.15,0.217],[0.183,0.25]>	<[0.683,0.783], [0.167,0.25], [0.217,0.317]>	<[0.667,0.767], [0.183,0.267], [0.233,0.333]>	<[0.7,0.767], [0.2,0.267], [0.233,0.3]>	<[0.667,0.767], [0.183,0.267], [0.233,0.333]>
A3	<[0.767,0.833], [0.133,0.183], [0.167,0.233]>	<[0.8,0.833], [0.167,0.16], [0.167,0.23]>	<[0.8,0.867], [0.1,0.167], [0.133,0.2]>	<[0.75,0.833], [0.117,0.2], [0.167,0.267]>	<[0.85,0.917], [0.05,0.1], [0.083,0.15]>	<[0.767,0.833], [0.133,0.2], [0.167,0.233]>
A4	<[0.667,0.767], [0.183,0.283], [0.233,0.333]>	<[0.8,0.867], [0.1,0.167], [0.133,0.2]>	<[0.7,0.75], [0.217,0.267], [0.25,0.317]>	<[0.733,0.783], [0.2,0.233], [0.217,0.283]>	<[0.75,0.833], [0.133,0.2], [0.167,0.267]>	<[0.767,0.85], [0.117,0.183], [0.15,0.25]>
A5	<[0.767,0.85], [0.117,0.183], [0.15,0.25]>	<[0.733,0.81], [0.133,0.21], [0.183,0.28]>	<[0.95,0.983], [0,0.017], [0.017,0.083]>	<[0.733,0.817], [0.15,0.217], [0.183,0.283]>	<[0.85,0.917], [0.067,0.1], [0.083,0.183]>	<[0.767,0.833], [0.133,0.2], [0.167,0.233]>

Step 3. After obtaining the aggregate matrix by taking the average of the expert opinions using Eq. (3), convert the IVN numbers into crisp values by using the score function in Eq. (2) as shown in Table 6.

Table 6. The crisp decision-matrix.

	C1	C2	C3	C4	C5	C6
A1	0.4375	0.45	0.6	0.383333	0.741667	0.370833
A2	0.5	0.6	0.525	0.491667	0.5	0.491667
A3	0.641666667	0.641667	0.7	0.629167	0.808333	0.633333
A4	0.483333333	0.7	0.479167	0.5375	0.620833	0.654167
A5	0.654166667	0.595833	0.95	0.5875	0.791667	0.633333

Step 4. When the relationship between the main criterion in our study C1 and other criteria was determined, it was calculated to reconsider the extent of agreement of the results. According to Table 7, experts rated C4 as +7, meaning that the impact on main criterion C1 of C4 is higher than average. Therefore, C4 moves its potential effect to +3, and so on. The higher order criterion takes part of the potential of the lower order criterion because the lower order criterion has less impact on the higher order criteria. The ranking of the first criterion is 1, and the ranking of the second criterion is 4. Consequently, some of the potential impacts of the second criterion should be transferred to the first criterion as Figure 3.

Table 7. Part of the potential impact criterion moves to the first main criterion.

Criteria	C1	C5	C3	C2	C4	C6
C1	---	+3	+6	+4	+7	+5
Criteria	C1	C5	C3	C2	C4	C6
C1	---	+7	+4	+6	+3	+5

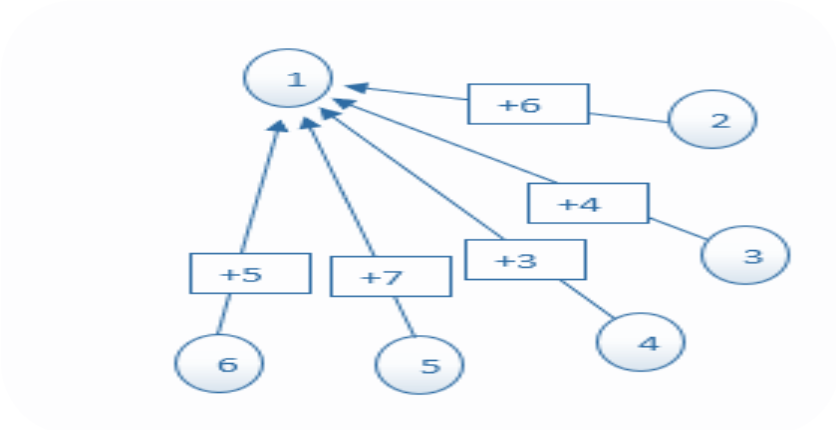

Figure 3. The relationship between the main criterion (C1) and the other system's criteria.

The criteria are ranked based on their importance and relationship. The plus or minus sign denotes the direction of the relationship according to Table 2, indicating that the criterion either impacts or depends upon the criterion of another system. As shown in Table 8 negative relationship indicates that the criterion under consideration is not as important as the criterion with which it is associated. Therefore, it allows her to reach some of her potential. Conversely, a positive correlation indicates that the criterion under consideration amplifies the potential of another criterion, thus increasing its impact potential.

Table 8. The matrix of the potential equilibrium.

	C1	C2	C3	C4	C5	C6
C1	0	7	4	6	3	5
C2	-7	0	-3	-1	-4	-2
C3	-4	3	0	2	-1	1
C4	-6	1	-2	0	-3	-1
C5	-3	4	1	3	0	2
C6	-5	2	-1	1	-2	0
Total	-25	17	-1	11	-7	5

Step 5. Table 9 shows the calculated potential equilibrium of the criteria, calculated the total potential impact using Eq. (6) based on the data presented in the first row of the matrix. When the total effect of dependence equals zero, the results of these calculations agree with each other.

Table 9. The results of the total effect (dependence) of the criteria.

	C1	C2	C3	C4	C5	C6	Total effect, (Dependence) p_j	p_j^f
C1	0	7	4	6	3	5	25	62
C2	-7	0	-3	-1	-4	-2	-17	20
C3	-4	3	0	2	-1	1	1	38
C4	-6	1	-2	0	-3	-1	-11	26
C5	-3	4	1	3	0	2	7	44
C6	-5	2	-1	1	-2	0	-5	32
Total	-25	17	-1	11	-7	5	0	222

Step 6. The weight was calculated using Eq. (8), and the FARE approach was used to analyze and evaluate the impact and relationship between cybersecurity measures in Industry 4.0, which produced a priority list of all possibilities considered. Then, the Delphi method was applied to verify the validity of these results.

w_j	0.279279	0.09009	0.171171	0.117117	0.198198	0.144144

Step 7. In our study, the Delphi approach was integrated with the FARE method to produce more exact results. Experts were requested to respond to questions in two rounds. The stakeholders present an anonymized summary of the expert opinions for the preceding round. Experts can evaluate their responses in light of feedback from other group experts. It is anticipated that, as a result of this process, an accepted response will emerge and the range of answers will narrow. A second round of surveys was conducted after the results of the calculations using the FARE approach. Stakeholders were able to evaluate their responses in light of additional professional comments in this way. This round's findings determine the accepted answer, and the process ends with a predetermined ending criterion according to the number of rounds or the stability of the results [31]. However, none of the participants indicated a desire to change what they contributed, and thus the study results were unchanged.

Step 8. Now the COBRA method in this study to calculate the final rank of the alternatives by applying the following steps. Establish the normalized decision matrix by applying Eq. (10) as shown in Table 10.

Table 10. The normalized decision matrix.

	C1	C2	C3	C4	C5	C6
	max	Min	max	max	min	Min
Weights	0.279279	0.09009	0.171171	0.117117	0.198198	0.144144
A1	0.66879	0.642857	0.631579	0.609272	0.917526	0.566879
A2	0.764331	0.857143	0.552632	0.781457	0.618557	0.751592
A3	0.980892	0.916667	0.736842	1	1	0.968153
A4	0.738854	1	0.504386	0.854305	0.768041	1
A5	1	0.85119	1	0.933775	0.979381	0.968153

As shown in Table 11, the weighted normalized decision matrix was obtained by applying Eq. (11).

Table 11. The weighted normalized decision matrix.

	C1	C2	C3	C4	C5	C6
	max	Min	max	max	min	Min
Weights	0.279279	0.09009	0.171171	0.117117	0.198198	0.144144
A1	0.186779	0.057915	0.108108	0.071356	0.181852	0.081712
A2	0.213462	0.07722	0.094595	0.091522	0.122597	0.108338
A3	0.273943	0.082583	0.126126	0.117117	0.198198	0.139554
A4	0.206346	0.09009	0.086336	0.100054	0.152224	0.144144
A5	0.279279	0.076684	0.171171	0.109361	0.194112	0.139554

To rank the alternatives as shown in Table 12, the distances of the positive ideal solutions and the distances of negative ideal solutions, the positive distances of the average solution and the negative distances of the average solution for each alternative were determined by Eq. (28) and the result shown in Figure 4.

Table 12. Ranking of the alternatives.

Alternatives	$d(PIS_j)_i$	$d(NIS_j)_i$	$d(AS_j)_i^+$	$d(AS_j)_i^-$	dC_i	RANK
A1	0.049054	0.029641	0.002914	0.025352	0.010463	1
A2	0.043338	0.034815	0.000596	0.02248	0.007602	3
A3	0.04111	0.038756	0.020218	0	-0.00447	4
A4	0.052706	0.022047	0.009332	0.017162	0.009622	2
A5	0.035104	0.05223	0.03087	0.000605	-0.01185	5

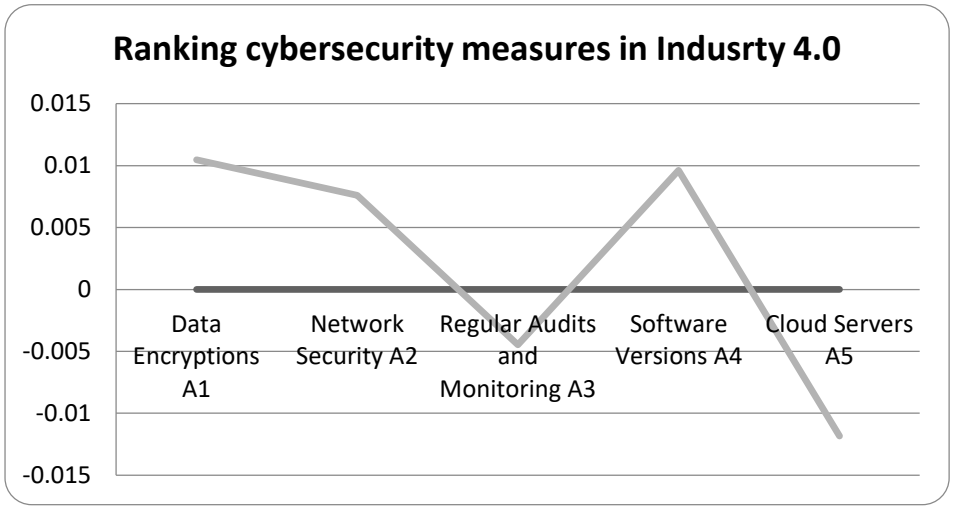

Figure 4. Ranking of the alternatives.

7 | Sensitivity Analysis

In this section we present sensitivity analysis which is useful for experts, alternatives, and criteria to prove the stability of the ranking of alternatives under specific cases, it has been carried out for the rank of alternatives. To assess the sensitivity of the solutions found in this study, six cases were created. In each case, the most significant weight criterion is 0.5, and the other criteria are equal the result appeared in Table 13.

Table 13. The result of the sensitivity analysis of the system.

Criteria	Original	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
Data Encryptions A1	0.010463	0.052491	−0.00279	0.040821	0.067362	0.027808	−0.00377
Network Security A2	0.007602	0.026921	0.016132	0.063771	0.016547	−0.00387	0.008393
Regular Audits and Monitoring A3	−0.00447	−0.04478	0.010116	−0.00499	−0.05631	0.01814	0.023182
Software Versions A4	0.009622	0.034346	0.028316	0.077971	−0.00399	0.005146	0.037809
Cloud Servers A5	−0.01185	−0.05429	−0.00584	−0.09404	−0.0439	0.011898	0.017355

As shown in Table 14 the alternatives are interchangeable, in the original case and Case 1 the rank of alternatives is equal but when the important weight criterion is in other cases the rank is exchanged. According to Table 14, Case 1 the increase in the weight of criterion 1 leads to this rank of alternatives $A1, A4, A2, A3, A5$. Case 2 the increase in the weight of criterion 2 leads to arranging the alternatives $A4, A2, A3, A1, A5$. Case 3 the increase in the weight of criterion 3 leads to arranging the alternatives $A4, A2, A1, A3, A5$. Case 4 the increase in the weight of criterion 4 leads to arranging the alternatives $A1, A2, A4, A5, A3$. Case 5 the increase in the weight of criterion 5 leads to arranging the alternatives $A1, A3, A5, A4, A2$. Case 6 the increase in the weight of criterion 6 leads to arranging the alternatives $A4, A3, A5, A2, A1$.

Table 14: The ranked alternatives in the cases of sensitivity analysis.

Criteria	Original	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
Data Encryptions A1	1	1	4	3	1	1	5
Network Security A2	3	3	2	2	2	5	4
Regular Audits and Monitoring A3	4	4	3	4	5	2	2
Software Versions A4	2	2	1	1	3	4	1
Cloud Servers A5	5	5	5	5	4	3	3

So, as shown in Figure 5 the weight differences become more significant which impacts the ranks of the alternatives.

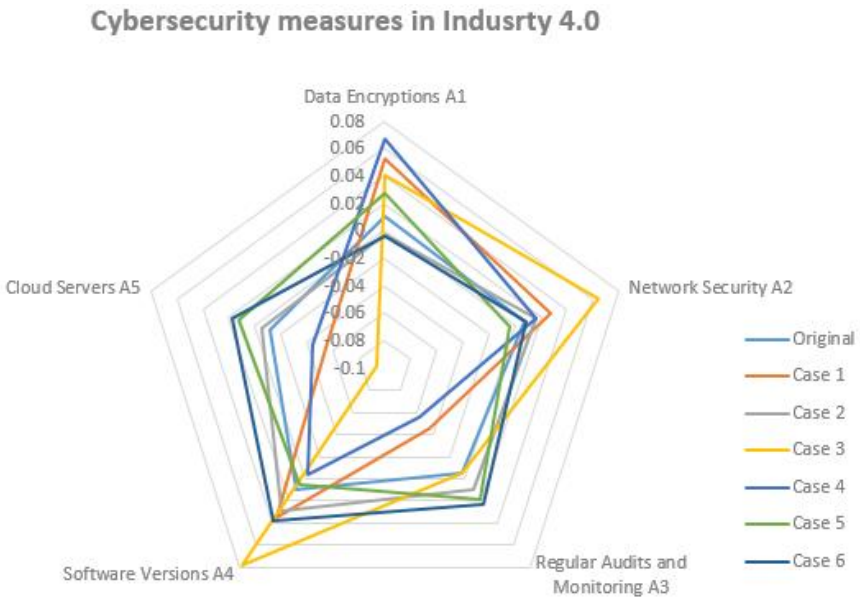

Figure 5. The ranked alternatives in the cases of sensitivity analysis.

8 | Comparative Analysis

In this section, we will conduct a comparison analysis to confirm the viability of the proposed decision-making method based on the rank of the alternatives. We compared the proposed method with other famous methods (i.e., PROMETHEE II [32], ARAS [33]). The experts have evaluated the second survey questionnaire using the COBRA method, which is used to evaluate each alternative measure concerning the criteria selected. The ranking process of the alternatives ratings where the best alternative is ranked "1", the good alternative is ranked "2", the fair alternative is ranked "3", the bad alternative is ranked "4", and the worst alternative is ranked "5". To obtain the result of Table 15 we compare the results of PROMETHEE II, ARAS methods with the result of the proposed method; we have used the same criteria and alternatives, and method of weight.

Table 15. Ranking of cybersecurity measures in the proposed study, PROMETHEE II, ARAS.

Alternatives	Proposed approach		PROMETHEE II		ARAS	
	dC_i	Rank	$\varphi(x)_i$	Rank	$S(x)_i$	Rank
Data Encryptions A1	0.010463	1	-0.13337	4	0.168841	5
Network Security A2	0.007602	3	0.047535	3	0.173095	4
Regular Audits and Monitoring A3	-0.00447	4	0.080594	2	0.229231	2
Software Versions A4	0.009622	2	-0.21833	5	0.18936	3
Cloud Servers A5	-0.01185	5	0.223568	1	0.239474	1

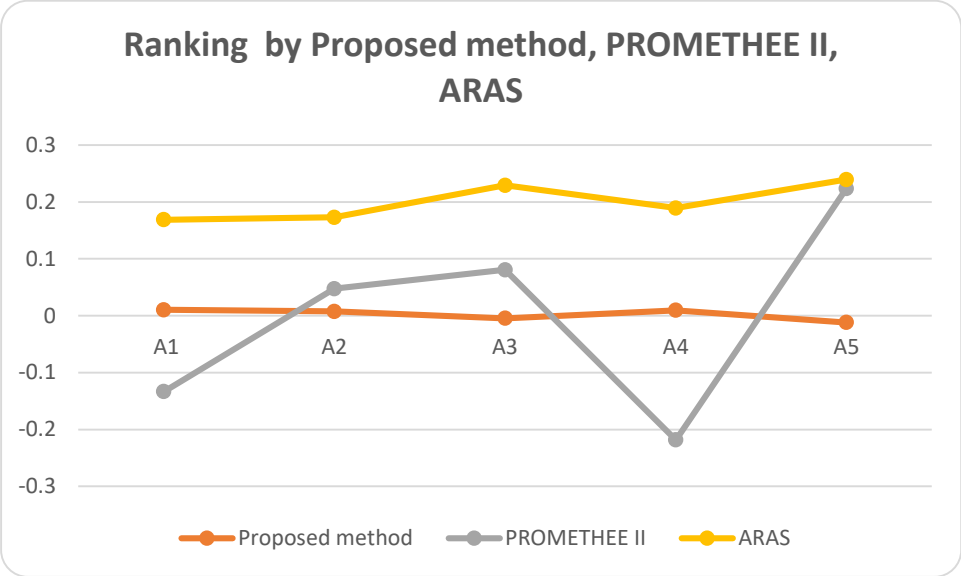

Figure 6. Ranking alternatives by COPRA, PROMETHEE II, ARAS.

After obtaining the result shown in Figure 6, we apply the Spearman correlation coefficient method [34] using Eq. (31) to determine whether two variables are correlated or not.

$$r_s = 1 - \frac{6.\sum_{j-1}^{m}(d_j)^2}{m.(m^2-1)} \tag{31}$$

Where m number of alternatives, d_j the difference between the ranks of the two methods.

r_s will set between $[-1, +1]$ and the strong correlation appears when the value is close to -1 (perfect negative correlation between all ranks), or $+1$ (perfect positive relationship between all ranks), and the weak correlation appears when the value is close to 0 (no correlation between all ranks). The result of Spearman correlation is equal to 0.999993533 between the proposed method and the PROMETHEE II method, and equal to 0.951130838 between the proposed method and ARAS method according to Eq. (31). There is a strong positive relationship between the alternative ranks obtained by the proposed method and the PROMETHEE II method, or the ARAS method. Based on the results obtained, the proposed method has good performance compared to other methods since it can handle uncertainty and simulate a natural decision-making process.

9 | Managerial Implications

This study aimed to assist stakeholders in choosing the most suitable cybersecurity measures of Industry 4.0 for ensuring sustainability in manufacturing based on environmental criteria and alternatives. The proposed approach is better than traditional approaches since it handles uncertainty, simulates natural decision-making, and then enables stakeholders and managers of smart factories to choose the most suitable cybersecurity measures. It also helps in reducing the threats to the network of factories.

10 | Conclusion

The fourth industrial revolution is also referred to as Industry 4.0. The first industrial revolution was the mechanical revolution that occurred in the 18th century with the invention of the steam engine and the train. Then came the second industrial revolution in the twentieth century as a result of the discovery of electrical energy. The third industrial revolution began in the 1970s with the launch of the digital computer and rapid automation. Then came Industry 4.0 which is about merging the physical, biological, and digital worlds due to the advancement of artificial intelligence and the Internet of Things. Industry 4.0 is supposed to represent a new era in intelligent and self-independent manufacturing. It more thoroughly combines communication, information, and intelligence technologies with manufacturing operations systems. With increasing number

of companies are depending on digital infrastructure, making cybersecurity a crucial problem. Governments all around the world have implemented cybersecurity measures for Industry 4.0 that aid in securing digital ecosystems and thwarting cyberattacks to safeguard sensitive data from online dangers.

During the decision-making process, a number of criteria led us to employ multicriteria decision-making procedures. The proposed study suggests a hybrid approach to decision-making, which is a combination of the MCDM approaches under the neutrosophic environment "IVNS-D-FARE-COPRA" method to prioritize cybersecurity measures in Industry 4.0 to achieve sustainable manufacturing during the implementation solutions of cybersecurity. The result showed that alternative one "Data Encryptions" is the best one, and alternative five "Cloud Servers" is the worst one. The influence of criteria weights on the ranking of the alternatives was examined in a sensitivity study to verify the model's stability. A comparative study was carried out to verify the model's performance and robustness with other models. In the future, we will be extending the framework to apply more criteria and alternatives and use other approaches for ranking the alternatives.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Author Contribution

All authors contributed equally to this work.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Kagermann, H., W.-D. Lukas, and W.J.V.n. Wahlster, Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution. 2011. 13(1): p. 2-3.

[2] Glistau, E. and N.I. Coello Machado. Industry 4.0, logistics 4.0 and materials-chances and solutions. in Materials Science Forum. 2018. Trans Tech Publ.

[3] Manavalan, E., K.J.C. Jayakrishna, and i. engineering, A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. 2019. 127: p. 925-953.

[4] Krstić, M., S. Tadić, and S.J.E.p. Zečević, Technological solutions in logistics 4.0. 2021. 69(5-6): p. 385-401.

[5] Sancho, J.C., A. Caro, M. Ávila, and A.J.F.G.C.S. Bravo, New approach for threat classification and security risk estimations based on security event management. 2020. 113: p. 488-505.

[6] Hofmann, E. and M.J.C.i.i. Rüsch, Industry 4.0 and the current status as well as future prospects on logistics. 2017. 89: p. 23-34.

[7] Saberi, S., M. Kouhizadeh, J. Sarkis, and L.J.I.j.o.p.r. Shen, Blockchain technology and its relationships to sustainable supply chain management. 2019. 57(7): p. 2117-2135.
[8] Müller, J.M., D. Kiel, and K.-I.J.S. Voigt, What drives the implementation of Industry 4.0? The role of opportunities and challenges in the context of sustainability. 2018. 10(1): p. 247.
[9] Götz, M. and J.J.K.N.U.V. Gracel, Przemysł czwartej generacji (Industry 4.0)–wyzwania dla badań w kontekście międzynarodowym. 2017(1 (51)): p. 217-235.
[10] Krstić, M., G.P. Agnusdei, P.P. Miglietta, S. Tadić, and V.J.S. Roso, Applicability of industry 4.0 technologies in the reverse logistics: a circular economy approach based on comprehensive distance based ranking (COBRA) method. 2022. 14(9): p. 5632.
[11] Aly, M., F. Khomh, and S.J.I.o.T. Yacout, What do practitioners discuss about iot and industry 4.0 related technologies? characterization and identification of iot and industry 4.0 categories in stack overflow discussions. 2021. 14: p. 100364.
[12] Amjad, M.S., M.Z. Rafique, M.A.J.S.P. Khan, and Consumption, Leveraging optimized and cleaner production through industry 4.0. 2021. 26: p. 859-871.
[13] Azeem, M., A. Haleem, S. Bahl, M. Javaid, R. Suman, and D.J.M.T.P. Nandan, Big data applications to take up major challenges across manufacturing industries: A brief review. 2022. 49: p. 339-348.
[14] Gao, Z., T. Wanyama, I. Singh, A. Gadhrri, and R.J.P.m. Schmidt, From industry 4.0 to robotics 4.0-a conceptual framework for collaborative and intelligent robotic systems. 2020. 46: p. 591-599.
[15] Gupta, S., R. Meissonier, V.A. Drave, and D.J.I.J.o.I.M. Roubaud, Examining the impact of Cloud ERP on sustainable performance: A dynamic capability view. 2020. 51: p. 102028.
[16] Iaiani, M., A. Tugnoli, S. Bonvicini, V.J.R.E. Cozzani, and S. Safety, Analysis of cybersecurity-related incidents in the process industry. 2021. 209: p. 107485.
[17] Kostrzewski, M.J.L., Securing of safety by monitoring of technical parameters in warehouse racks, in high-bay warehouses and high storage warehouses-literature review of the problem. 2017. 13(2).
[18] Ng, T.C., S.Y. Lau, M. Ghobakhloo, M. Fathi, and M.S.J.S. Liang, The application of industry 4.0 technological constituents for sustainable manufacturing: A content-centric review. 2022. 14(7): p. 4327.
[19] Lepore, D., A. Micozzi, and F.J.S. Spigarelli, Industry 4.0 accelerating sustainable manufacturing in the COVID-19 era: assessing the readiness and responsiveness of Italian regions. 2021. 13(5): p. 2670.
[20] Torbacki, W.J.S., A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. 2021. 13(16): p. 8833.
[21] Tanaji, B.A. and S.J.A.S.C. Roychowdhury, BWM Integrated VIKOR method using Neutrosophic fuzzy sets for cybersecurity risk assessment of connected and autonomous vehicles. 2024. 159: p. 111628.
[22] Toussaint, M., S. Krima, and H.J.J.o.I.I.I. Panetto, Industry 4.0 data security: a cybersecurity frameworks review. 2024: p. 100604.
[23] Wang, H., F. Smarandache, R. Sunderraman, and Y.-Q. Zhang, interval neutrosophic sets and logic: theory and applications in computing: Theory and applications in computing. Vol. 5. 2005: Infinite Study.
[24] Yang, L., M. Zhao, J. Shao, and Y.J.A.a.S. Chen, A Multi-Criteria Approach for Supplier Evaluation Considering Transparency Under Information Described by Interval-Valued Neutrosophic Sets.
[25] Ginevičius, R.J.I.J.o.I.T. and D. Making, A new determining method for the criteria weights in multicriteria evaluation. 2011. 10(06): p. 1067-1095.
[26] Qadir, F., A. Khalid, S. Haqqani, and G.J.B.p.h. Medhin, The association of marital relationship and perceived social support with mental health of women in Pakistan. 2013. 13: p. 1-13.
[27] Roy, J., D. Pamučar, and S.J.A.o.O.R. Kar, Evaluation and selection of third party logistics provider under sustainability perspectives: an interval valued fuzzy-rough approach. 2020. 293: p. 669-714.
[28] Dalkey, N. and O.J.M.s. Helmer, An experimental application of the Delphi method to the use of experts.1963.9(3): p.458-467.
[29] Pojadas, D.J., M.L.S.J.I.J.o.M. Abundo, and D. Making, A web-based Delphi multi-criteria group decision-making framework for renewable energy project development processes. 2020. 19(4): p. 426-449.
[30] Zha, S., Y. Guo, S. Huang, and S.J.M.P.i.E. Wang, A hybrid MCDM method using combination weight for the selection of facility layout in the manufacturing system: A case study. 2020. 2020: p. 1-16; Zhao, H., S. Guo, and H.J.E. Zhao, Comprehensive assessment for battery energy storage systems based on fuzzy-MCDM considering risk preferences. 2019. 168: p. 450-461.
[31] Karabasevic, D., D. Stanujkic, S. Urosevic, G. Popovic, M.J.M.J.o.S.B. Maksimovic, and M.S.i.E. Economies, An approach to criteria weights determination by integrating the Delphi and the adapted SWARA methods. 2017. 22(3): p. 15-25.
[32] Brans, J.-P. and P.J.M.s. Vincke, Note—A Preference Ranking Organisation Method: (The PROMETHEE Method for Multiple Criteria Decision-Making). 1985. 31(6): p. 647-656.
[33] Zavadskas, E.K., Z.J.T. Turskis, and e.d.o. economy, A new additive ratio assessment (ARAS) method in multicriteria decision-making. 2010. 16(2): p. 159-172.
[34] Raju, K.S. and D.N.J.A.S. Kumar, Multicriterion decision making in irrigation planning. 1999. 62(2): p. 117-129.

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.