An efficient intrusion detection model based on neutrosophic logic for optimal response from the arranged response set

Ali Alqazzaz[1*], Ibrahim Alrashdi[2]
[1]Department of Information Systems and Cybersecurity, College of Computing and Information Technology, University of Bisha, P.O. Box 344, Bisha 61922, Saudi Arabia
[2]Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka 2014, Saudi Arabia
Emails: aqzaz@ub.edu.sa; irrashdi@ju.edu.sa

Abstract
While an Automated Intrusion Response System (AIRS) chooses and initiates a suitable reaction from the pool of response groups based on specific response choice requirements to reduce the intrusion immediately, an Intrusion Detection System (IDS) finds the intrusions and generates alerts. The accurate assessment of the critical weight of all responses chosen and the prioritization of the incursion response set are the biggest hurdles when creating an AIRS. This study suggested a multi-criteria decision-making (MCDM) method for ranking intrusion responses. The TOPSIS method is an MCDM method used to rank the alternatives. The TOPSIS method integrated with the single-valued neutrosophic set (SVNS) to overcome uncertainty. This study used 16 criteria and 10 alternatives to be evaluated by experts and decision-makers. The sensitivity analysis shows the rank of other options under different cases. The criteria weights are changed under 17 cases. The results of sensitivity analysis show the rank of alternatives is stable. The suggested method was compared with other MCDM methods to show its effectiveness and robustness.

Keywords: Intrusion Detection System; Security; Multi-Criteria Decision Making; Neutrosophic Logic; Intrusion Response.

1. Introduction

The increased reliance on Internet services has led to a rapid rise in infiltration risks. The PWC Global State of Information Security Survey 2016 reports that there has been a 38% rise in intrusion events over the previous year. A robust defense mechanism is required to prevent organizational loss due to increased occurrences. IDS looks for intruders, finds them, and sends the network administrator notifications. The network administrator manually chooses the best answer using the organization's security policy and response selection criteria. Because the IDS generates a lot of warnings, it takes a lot of effort for the network administrator to review each alert and decide on the best course of action quickly[1], [2]. The time the administrator takes to determine the proper action in response to a specific warning directly correlates with how long the attacker compromises the target system. Because of this, an automated intrusion response system is needed to quickly choose and initiate the appropriate reaction, preventing the attacker from having additional time to compromise the target system. To neutralize the assault with the least penalty cost, an AIRS aims to choose the appropriate reaction for the warnings automatically. Several models and frameworks are suggested for the AIRS, considering different answer selection criteria. Four answer selection criteria that the different domain researchers most often use are discovered and chosen in this work[3]–[5].

The main challenge is determining the precise quantitative relevance weight for every criterion so that the correct answer may be chosen. According to the literature review, most of the AIRS models in use manually assigned a weight to each criterion without doing more research. It should be possible to solve this issue in a well-defined manner. Prioritizing the set of replies by the specified criteria is another challenging task that must be completed before the AIRS can choose the best response[6]–[8].

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

The Decision Maker (DM) chooses the best option based on several factors. It is necessary to comprehend the issue to rank the solution mathematically. Multi-criteria decision-making (MCDM) may be helpful in this situation[9]–[12]. When making decisions, it might be challenging to determine which different answer to rank or pick optimally since it relies on several competing factors[13]–[15]. Finding the weight of the criteria is a significant component of the DMs. Integrating decision experts' opinions into linguistic grading is the initial phase in the decision-making process. The decision experts may take doubt, reluctance, and ambiguity into account. Therefore, the language evaluation may only sometimes be converted to a set scale. In this scenario, the researchers must resolve the response ranking issue using MCDM approaches in a reluctant, unclear setting[16]–[18]. Fuzzy Sets (FS) theories are useful for handling unclear or inconsistent data, but they could be better at handling other types of information[19]–[21]. Therefore, sophisticated computational tools such as Intuitionistic Fuzzy Sets (IFSs) and Neutrosophic Sets (NSs), are a generalization of FSs[22]–[24].

Whether the total of the single-valued neutrosophic components is less than 1, greater than 1, or equal to 1, NS is an extension of IFS. When applying the neutrosophic aggregation operators to the case where the sum of the components is 1 as in IFS, the results differ from those obtained when applying the intuitionistic fuzzy operators because the latter ignore indeterminacy, whereas the former take it into account on the same level as truth-membership and falsehood-non-membership. In addition to handling independent components, NS is also more adaptable and efficient than IFS since it can also handle partially dependent and partially independent components [22]. In this work, we handle our intrusion detection model using the NS to ensure the best possible response from the arranged response set.

1.1 Intrusion Response System

When an attack is identified, intrusion response systems respond differently to minimize its impact on the system under protection. Despite its obstacles, difficulties, and limits, developing sophisticated autonomous intrusion response systems has lately attracted much attention in light of this survey research. This is because new security needs are imposed by the open, unsecured nature of device connection in critical infrastructures today. These requirements may be met by using the advantages of autonomous intrusion response systems. One of the automated IRS's advantages is that it can operate without human assistance, so there won't be any waiting between discovering an assault and taking appropriate action[25]–[27]. Another advantage is that they may be used for various infrastructures. Additionally, with their recent advancements in applying reinforcement learning solution techniques, they can handle the prevalent scalability problem. Furthermore, automated IRS respond in a way that is flexible and adaptable to the circumstances of the present situation. Real-time response to various assault situations is another crucial component of autonomous IRS. Additionally, automated IRS saves time and effort by eliminating the need for human investigations of various security breaches. Lastly, installing an automatic IRS may minimize reaction risk and expense while safeguarding your system from unavoidable assaults[28]–[30]. Based on intrusion detection system (IDS) warnings, an intrusion response system (IRS) continually checks the system's health to enable efficient handling of malicious or unauthorized activity. This involves taking the necessary steps to stop issues from worsening and restore the system to a healthy state. A notification system generates alerts upon detection of an assault. Information such as the attack description, attack time, source IP address, and user accounts utilized in the attack may all be included in an alert. Depending on the kind of assault, an IRS automatically carries out a predetermined set of reaction activities. Unlike intrusion detection systems (IDS), which need human involvement after intrusion detection, an automated technique doesn't require human intervention[31]–[33].

The rest of this paper is organized as follows: section 2 presents the suggested methodology under SVNS. Section 3 presented the results of this study. Section 4 presented the sensitivity analysis. Section 5 presented the comparative analysis. Section 6 presented the managerial implications. Section 7 presented the conclusions of this study.

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

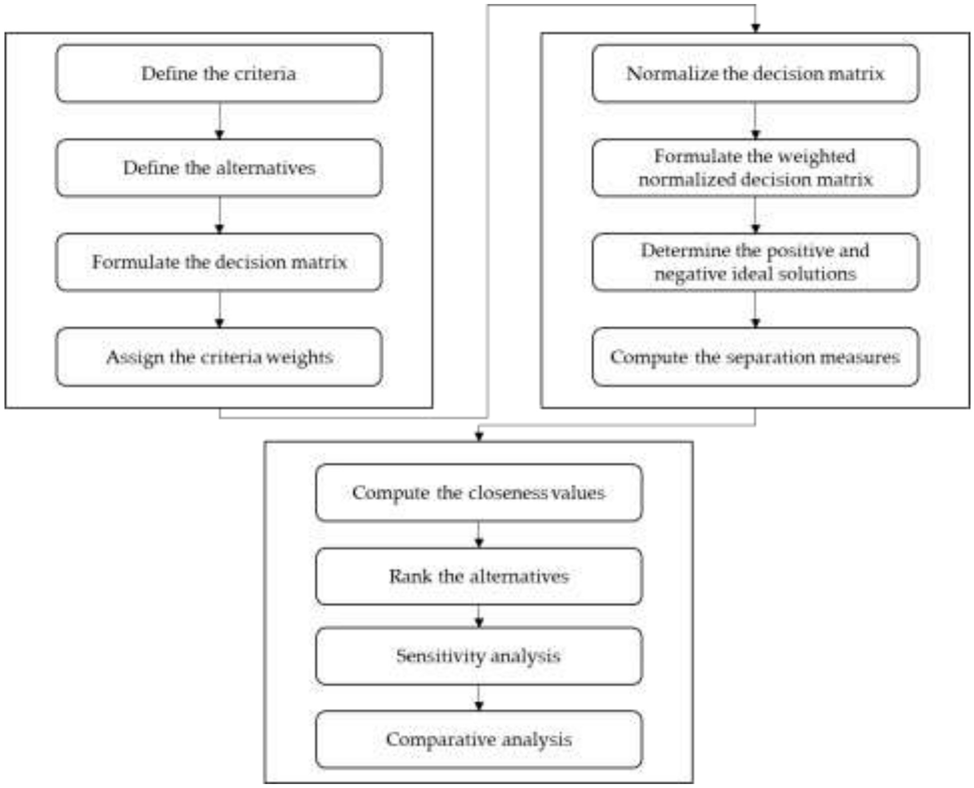

Figure 1: The steps of the SVN-TOPSIS method.

1.2 Preliminaries

Florentin Smarandache invented the neutrosophic theory in 1998. Definitions of single-valued neutrosophic sets, trapezoidal neutrosophic numbers, and neutrosophic sets are presented. [22].

Definition 1 Let X be a space of points and $x \in X$. A neutrosophic set A in X is defined by a truth-membership function $T_A(x)$, an indeterminacy-membership function $I_A(x)$ and a falsity-membership function $F_A(x)$, $T_A(x)$, $I_A(x)$ and $F_A(x)$ are real standard or real nonstandard subsets of]-0, 1+[. That is $T_A(x)$:X→]-0, 1+[$I_A(x)$:X→]-0, 1+[and $F_A(x)$:X→]-0, 1+[. There is no restriction on the sum of $T_A(x)$, $I_A(x)$ and $F_A(x)$, so 0− ≤ sup (x) + sup x ≤3+.

Definition 2 Let X be a discourse universe. An object of the form A={⟨x, $T_A(x)$, $I_A(x)$, $F_A(x)$,⟩:$x \in X$}, is a single-valued neutrosophic set A over X, where $T_A(x)$:X→ [0,1], $I_A(x)$:X→ [0,1] and $F_A(x)$:X→[0,1] with 0≤ $T_A(x)$ + $I_A(x)$ + $F_A(x)$ ≤3 for all $x \in X$. The intervals $T_A(x)$, $I_A(x)$ and $F_A(x)$ represent the truth-membership degree, the indeterminacy-membership degree, and the falsity membership degree of x to A, respectively. For convenience, a Single Valued Neutrosophic (SVN) number is represented by A= (a, b, c), where a, b, $c \in$ [0, 1] and a+b+c≤3.

Definition 3 Let $\alpha_{\tilde{a}}$, $\theta_{\tilde{a}}$, $\beta_{\tilde{a}}$ ϵ [0,1]and a_1 , a_2 , a_3 , a_4ϵ R, where $a_1 \le a_2 \le a_3 \le a_4$. Then, a single-valued trapezoidal neutrosophic number $\tilde{a}$=⟨(a_1 , a_2 , a_3, a_4); $\alpha_{\tilde{a}}$, $\theta_{\tilde{a}}$, $\beta_{\tilde{a}}$⟩ is a special neutrosophic set on the real line set R, whose truth-membership, indeterminacy-membership, and falsity-membership functions are defined as:

$$T_{\tilde{a}}(x) = \begin{cases} \alpha_{\tilde{a}}\left(\frac{x-a_1}{a_2-a_1}\right) & (a_1 \le x \le a_2) \\ \alpha_{\tilde{a}} & (a_2 \le x \le a_3) \\ \alpha_{\tilde{a}}\left(\frac{a_4-x}{a_4-a_3}\right) & (a_3 \le x \le a_4) \\ 0 & otherwise. \end{cases}$$

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

$$I_{\tilde{a}}\ (x) = \begin{cases} \frac{(a_2 - x + \theta_{\tilde{a}}(x-a_1))}{(a_2-a_1)} & (a_1 \le x \le a_2) \\ \alpha_{\tilde{a}} & (a_2 \le x \le a_3) \\ \frac{(x-a_3+\theta_{\tilde{a}}(a4-x))}{(a_4-a_3)} & (a_3 \le x \le a_4) \\ 1 & otherwise. \end{cases} ,$$

$$F_{\tilde{a}}\ (x) = \begin{cases} \frac{(a_2 - x + \beta_{\tilde{a}}(x-a_1))}{(a_2-a_1)} & (a_1 \le x \le a_2) \\ \alpha_{\tilde{a}} & (a_2 \le x \le a_3) \\ \frac{(x-a_3+\beta_{\tilde{a}}(a4-x))}{(a_4-a_3)} & (a_3 \le x \le a_4) \\ 1 & otherwise. \end{cases}$$

The maximum truth-membership degree, minimum indeterminacy-membership degree, and minimum falsity-membership degree are represented by the symbols $\alpha_{\tilde{a}}$, $\theta_{\tilde{a}}$ and $\beta_{\tilde{a}}$, respectively.

2. The proposed Approach

This section introduces the TOPSIS method under single valued neutrosophic sets to overcome uncertainty[34], [35]. The TOPSIS method is used to rank the alternatives. TOPSIS method is used under single-valued neutrosophic numbers (SVNNs) to evaluate the criteria and alternatives[36], [37]. The steps of the TOPSIS method are shown in Figure 1. The following are the steps of the suggested methodology:

Step 1. Devise the decision matrix. Construction of a decision matrix between criteria and alternatives as

$$X = \begin{bmatrix} x_{11} & \cdots & x_{1m} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nm} \end{bmatrix} \tag{1}$$

Where n refers to the number of alternatives (ith) and n refers to the number of criteria (jth)

This study used the SVNNs as shown in Table 1

Table 1: Single valued neutrosophic scale.

Linguistic Variables	SVNNs
Extremely High Importance	(0.9,0.1,0.1)
Very High Importance	(0.8,0.2,0.15)
High Importance	(0.7,0.3,0.2)
Moderate Importance	(0.6,0.4,0.3)
Equal Importance	(0.5,0.5,0.5)
Low Importance	(0.4,0.6,0.55)
Very Low Importance	(0.3,0.7,0.6)
Very Very Low Importance	(0.2,0.8,0.7)
Extremely Low Importance	(0.1,0.9,0.8)

Step 2. Appoint the criteria weights. The criteria weights are computed by using the average method where $\sum_{j=1}^{m} w_j = 1$.

Step 3. Normalize the decision matrix as

$$y_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{n} x_{ij}^2}} \tag{2}$$

$$Y = \begin{bmatrix} y_{11} & \cdots & y_{1m} \\ \vdots & \ddots & \vdots \\ y_{n1} & \cdots & y_{nm} \end{bmatrix} \tag{3}$$

Step 4. Formulate the weighted normalized decision matrix.

$$u_{ij} = w_j y_{ij} \tag{4}$$

Step 5. Conclude the positive and negative ideal solutions as

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

$$u^{+} = \left\{\begin{matrix} \left(\max_{i} u_{ij}\, j \in C_b\right) . \\ \left(\min_{i} u_{ij}\, j \in C_c\right) . \\ j = 1,2, \dots, m \end{matrix}\right\} = (u_1^{+}, u_2^{+}, \dots, u_m^{+}) \quad (5)$$

$$u^{-} = \left\{\begin{matrix} \left(\min_{i} u_{ij}\, j \in C_b\right) . \\ \left(\max_{i} u_{ij}\, j \in c\right) . \\ j = 1,2, \dots, m \end{matrix}\right\} = (u_1^{-}, u_2^{-}, \dots, u_m^{-}) \quad (6)$$

Where C_b refers to the positive criteria and C_c refers to the negative criteria

Step 6. Compute the separation measures.

$$d_i^{+} = \sqrt{\sum_{j=1}^{m} \left(u_{ij} - u^{+}\right)^2} \quad (7)$$

$$d_i^{-} = \sqrt{\sum_{j=1}^{m} \left(u_{ij} - u^{-}\right)^2} \quad (8)$$

Step 7. Compute the closeness values

$$L_i = \frac{d_i^{-}}{d_i^{-} + d_i^{+}} \quad (9)$$

Figure 2: The intrusion criteria

3. Results and Discussions

This section introduces the results of the suggested method for ranking intrusion response using the TOPSIS method. This study used 16 criteria and 10 alternatives. Figure 2 shows the criteria used in this study.

Step 1. Formulate the decision matrix by using Eq. (1) as shown in Table 2. The SVNNs are shown in Table 1. The experts evaluate the criteria and alternatives by using SVNNs.

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

Table 2: Decision matrix by the first expert.

	IDR_1	IDR_2	IDR_3	IDR_4	IDR_5	IDR_6	IDR_7	IDR_8	IDR_9	IDR_{10}
IRC_1	(0.2,0.8,0.7)	(0.5,0.5,0.5)	(0.3,0.7,0.6)	(0.6,0.4,0.3)	(0.9,0.1,0.1)	(0.5,0.5,0.5)	(0.9,0.1,0.1)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.3,0.7,0.6)
IRC_2	(0.2,0.8,0.7)	(0.6,0.4,0.3)	(0.3,0.7,0.6)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.3,0.7,0.6)	(0.5,0.5,0.5)	(0.1,0.9,0.8)
IRC_3	(0.3,0.7,0.6)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.1,0.9,0.8)	(0.3,0.7,0.6)	(0.5,0.5,0.5)	(0.9,0.1,0.1)	(0.9,0.1,0.1)	(0.5,0.5,0.5)	(0.5,0.5,0.5)
IRC_4	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.4,0.6,0.55)	(0.9,0.1,0.1)	(0.4,0.6,0.55)	(0.6,0.4,0.3)	(0.2,0.8,0.7)
IRC_5	(0.8,0.2,0.15)	(0.3,0.7,0.6)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.8,0.2,0.15)	(0.4,0.6,0.55)	(0.8,0.2,0.15)	(0.9,0.1,0.1)
IRC_6	(0.4,0.6,0.55)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.8,0.2,0.15)	(0.7,0.3,0.2)	(0.8,0.2,0.15)	(0.4,0.6,0.55)	(0.8,0.2,0.15)
IRC_7	(0.3,0.7,0.6)	(0.3,0.7,0.6)	(0.6,0.4,0.3)	(0.2,0.8,0.7)	(0.4,0.6,0.55)	(0.9,0.1,0.1)	(0.9,0.1,0.1)	(0.2,0.8,0.7)	(0.5,0.5,0.5)	(0.4,0.6,0.55)
IRC_8	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.1,0.9,0.8)	(0.5,0.5,0.5)	(0.7,0.3,0.2)	(0.1,0.9,0.8)	(0.6,0.4,0.3)	(0.3,0.7,0.6)	(0.8,0.2,0.15)
IRC_9	(0.9,0.1,0.1)	(0.9,0.1,0.1)	(0.4,0.6,0.55)	(0.5,0.5,0.5)	(0.8,0.2,0.15)	(0.8,0.2,0.15)	(0.7,0.3,0.2)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.5,0.5,0.5)
IRC_{10}	(0.5,0.5,0.5)	(0.7,0.3,0.2)	(0.5,0.5,0.5)	(0.9,0.1,0.1)	(0.8,0.2,0.15)	(0.5,0.5,0.5)	(0.8,0.2,0.15)	(0.5,0.5,0.5)	(0.9,0.1,0.1)	(0.9,0.1,0.1)
IRC_{11}	(0.4,0.6,0.55)	(0.9,0.1,0.1)	(0.6,0.4,0.3)	(0.7,0.3,0.2)	(0.4,0.6,0.55)	(0.2,0.8,0.7)	(0.4,0.6,0.55)	(0.6,0.4,0.3)	(0.8,0.2,0.15)	(0.4,0.6,0.55)
IRC_{12}	(0.3,0.7,0.6)	(0.8,0.2,0.15)	(0.6,0.4,0.3)	(0.8,0.2,0.15)	(0.9,0.1,0.1)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.6,0.4,0.3)	(0.8,0.2,0.15)
IRC_{13}	(0.8,0.2,0.15)	(0.9,0.1,0.1)	(0.5,0.5,0.5)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.2,0.8,0.7)	(0.6,0.4,0.3)	(0.6,0.4,0.3)	(0.5,0.5,0.5)	(0.5,0.5,0.5)
IRC_{14}	(0.7,0.3,0.2)	(0.6,0.4,0.3)	(0.6,0.4,0.3)	(0.9,0.1,0.1)	(0.5,0.5,0.5)	(0.9,0.1,0.1)	(0.3,0.7,0.6)	(0.5,0.5,0.5)	(0.6,0.4,0.3)	(0.8,0.2,0.15)
IRC_{15}	(0.6,0.4,0.3)	(0.6,0.4,0.3)	(0.9,0.1,0.1)	(0.5,0.5,0.5)	(0.3,0.7,0.6)	(0.4,0.6,0.55)	(0.3,0.7,0.6)	(0.1,0.9,0.8)	(0.6,0.4,0.3)	(0.2,0.8,0.7)
IRC_{16}	(0.9,0.1,0.1)	(0.5,0.5,0.5)	(0.4,0.6,0.55)	(0.9,0.1,0.1)	(0.2,0.8,0.7)	(0.2,0.8,0.7)	(0.5,0.5,0.5)	(0.6,0.4,0.3)	(0.7,0.3,0.2)	(0.4,0.6,0.55)

Step 2. Assign the criteria weights as shown in Figure 3.

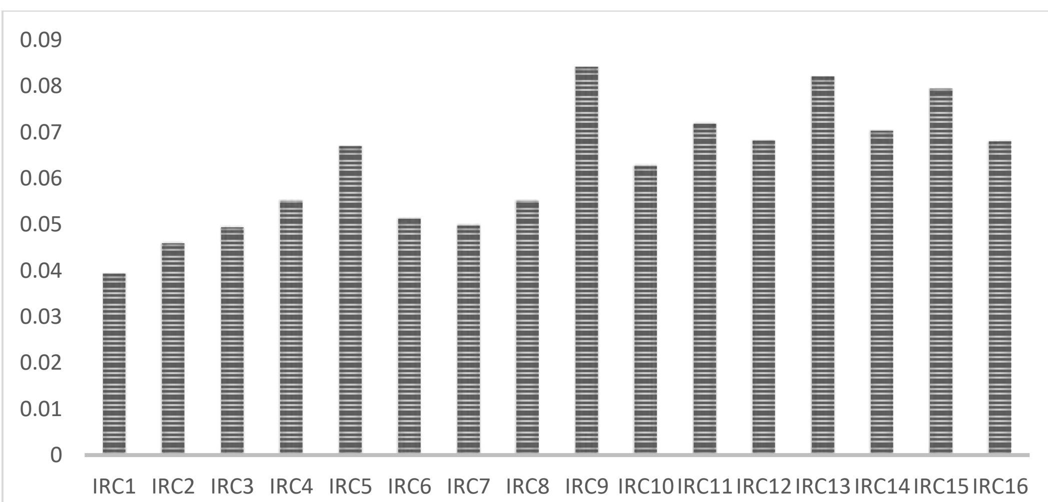

Figure 3: The criteria of intrusion response weights.

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

Table 3: Normalized decision matrix.

	IDR_1	IDR_2	IDR_3	IDR_4	IDR_5	IDR_6	IDR_7	IDR_8	IDR_9	IDR_{10}
IRC_1	0.119782	0.269254	0.18684	0.32505	0.493974	0.269254	0.493974	0.323515	0.269254	0.18684
IRC_2	0.167225	0.45595	0.235161	0.343596	0.343596	0.414797	0.343596	0.24104	0.343596	0.080347
IRC_3	0.192368	0.279518	0.279518	0.065362	0.173237	0.279518	0.524494	0.512803	0.279518	0.279518
IRC_4	0.283952	0.283952	0.283952	0.376803	0.283952	0.244004	0.531734	0.246163	0.341174	0.1274
IRC_5	0.389745	0.164822	0.317806	0.239493	0.248599	0.239493	0.389745	0.217638	0.389745	0.438463
IRC_6	0.196748	0.249372	0.249372	0.299625	0.258853	0.405821	0.353197	0.424311	0.216185	0.404873
IRC_7	0.195811	0.195811	0.374455	0.135726	0.222634	0.519301	0.528421	0.14431	0.282182	0.256432
IRC_8	0.302354	0.302354	0.302354	0.070702	0.302354	0.428238	0.071852	0.392025	0.212107	0.492043
IRC_9	0.416466	0.418542	0.206677	0.226134	0.370115	0.371412	0.322121	0.27456	0.227431	0.227431
IRC_{10}	0.215499	0.305222	0.215499	0.403548	0.351927	0.215499	0.349878	0.215499	0.395354	0.394535
IRC_{11}	0.229543	0.487276	0.318139	0.395156	0.229543	0.128866	0.208904	0.318139	0.430897	0.229543
IRC_{12}	0.175654	0.376907	0.308057	0.38794	0.425896	0.232146	0.232146	0.232146	0.308057	0.379114
IRC_{13}	0.416656	0.468168	0.255135	0.319646	0.255135	0.124172	0.338563	0.338563	0.255135	0.255135
IRC_{14}	0.33012	0.280048	0.281377	0.428934	0.233078	0.437353	0.161737	0.233078	0.281377	0.379704
IRC_{15}	0.38139	0.377912	0.559334	0.30488	0.188956	0.264307	0.186058	0.071293	0.376753	0.13679
IRC_{16}	0.486936	0.265418	0.230096	0.485927	0.132709	0.119085	0.265418	0.320419	0.381476	0.230096

Table 4: The weighted normalized decision matrix

	IDR_1	IDR_2	IDR_3	IDR_4	IDR_5	IDR_6	IDR_7	IDR_8	IDR_9	IDR_{10}
IRC_1	0.007427	0.016694	0.011584	0.020153	0.030626	0.016694	0.030626	0.020058	0.016694	0.011584
IRC_2	0.010368	0.028269	0.01458	0.021303	0.021303	0.025717	0.021303	0.014944	0.021303	0.004981
IRC_3	0.011927	0.01733	0.01733	0.004052	0.010741	0.01733	0.032519	0.031794	0.01733	0.01733
IRC_4	0.017605	0.017605	0.017605	0.023362	0.017605	0.015128	0.032968	0.015262	0.021153	0.007899
IRC_5	0.024164	0.010219	0.019704	0.014849	0.015413	0.014849	0.024164	0.013494	0.024164	0.027185
IRC_6	0.012198	0.015461	0.015461	0.018577	0.016049	0.025161	0.021898	0.026307	0.013403	0.025102
IRC_7	0.01214	0.01214	0.023216	0.008415	0.013803	0.032197	0.032762	0.008947	0.017495	0.015899
IRC_8	0.018746	0.018746	0.018746	0.004384	0.018746	0.026551	0.004455	0.024306	0.013151	0.030507

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

IRC_9	0.025821	0.02595	0.012814	0.01402	0.022947	0.023028	0.019972	0.017023	0.014101	0.014101
IRC_{10}	0.013361	0.018924	0.013361	0.02502	0.021819	0.013361	0.021692	0.013361	0.024512	0.024461
IRC_{11}	0.014232	0.030211	0.019725	0.0245	0.014232	0.00799	0.012952	0.019725	0.026716	0.014232
IRC_{12}	0.010891	0.023368	0.0191	0.024052	0.026406	0.014393	0.014393	0.014393	0.0191	0.023505
IRC_{13}	0.025833	0.029026	0.015818	0.019818	0.015818	0.007699	0.020991	0.020991	0.015818	0.015818
IRC_{14}	0.020467	0.017363	0.017445	0.026594	0.014451	0.027116	0.010028	0.014451	0.017445	0.023542
IRC_{15}	0.023646	0.023431	0.034679	0.018903	0.011715	0.016387	0.011536	0.00442	0.023359	0.008481
IRC_{16}	0.034086	0.018579	0.016107	0.034015	0.00929	0.008336	0.018579	0.022429	0.026703	0.016107

Step 3. Normalize the decision matrix by using Eqs. (2 and 3) as shown in Table 3.
Step 4. Formulate the weighted normalized decision matrix by using Eq. (4) as shown in Table 4
Step 5. Determine the positive and negative ideal solutions by using Eqs. (5 and 6). All criteria are positive.
Step 6. Compute the separation measures by using Eqs. (7 and 8).
Step 7. Compute the closeness values by using Eq. (9) as shown in Figure 4. Alternative 7 is the best and alternative 10 is the worst. Table 5 shows the advantages and disadvantages of intrusion-based neutrosophic sets and classical sets.

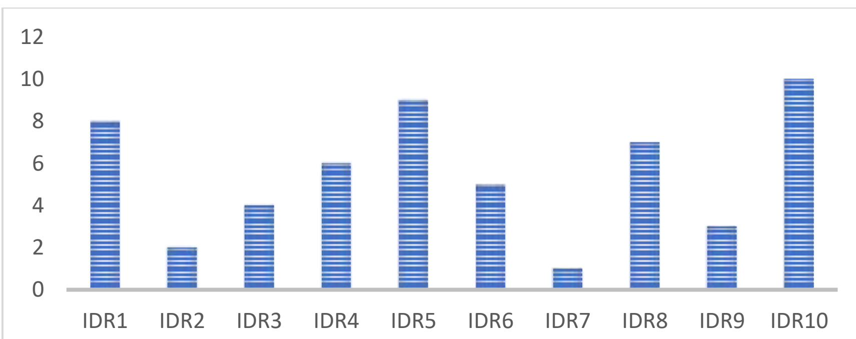

Figure 4: The rank of alternatives is based on closeness by the TOPSIS method.

Table 5: Advantages and disadvantages of intrusion detection based on neutrosophic set and classical approach.

Linguistic Variables	intrusion detection based on neutrosophic set	intrusion detection based on classical set
Advantage	It has three membership degrees. It has an indeterminacy value. Overcome uncertainty and vague data. It has truth, indeterminacy, and falsity degrees	-
Dis-advantage	-	Cannot deal with uncertainty. It cannot deal with uncertainty. It has one value

4. Sensitivity Study

This section shows the rank of alternatives under sensitivity analysis. The criteria weights are changed under sensitivity analysis with 17 cases. In the first, the criteria weights are equal. Then, the first criterion is put with 0.07, and the other criteria are equal. The criteria weights are shown in Figure 5. Then, the closeness values are computed

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

by the single-valued neutrosophic TOPSIS method, as shown in Figure 6. The rank of alternatives is shown in Figure 7. The sensitivity analysis results show alternative 7 is the best in all cases. Alternative 10 is the worst in all cases except 6, 9, 15. Alternative 5 is the worst in cases 6, 9, and 15.

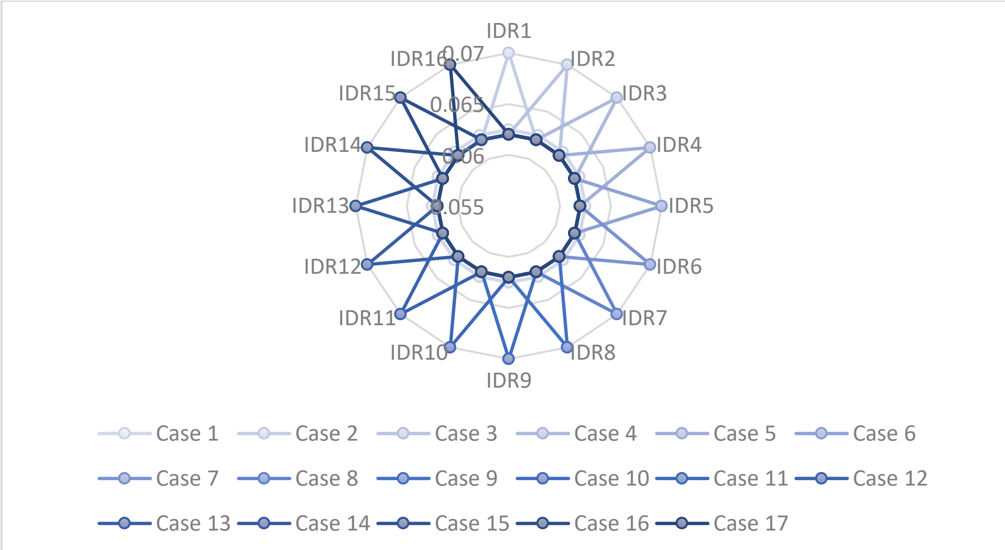

Figure 5: The criteria weights under sensitivity analysis.

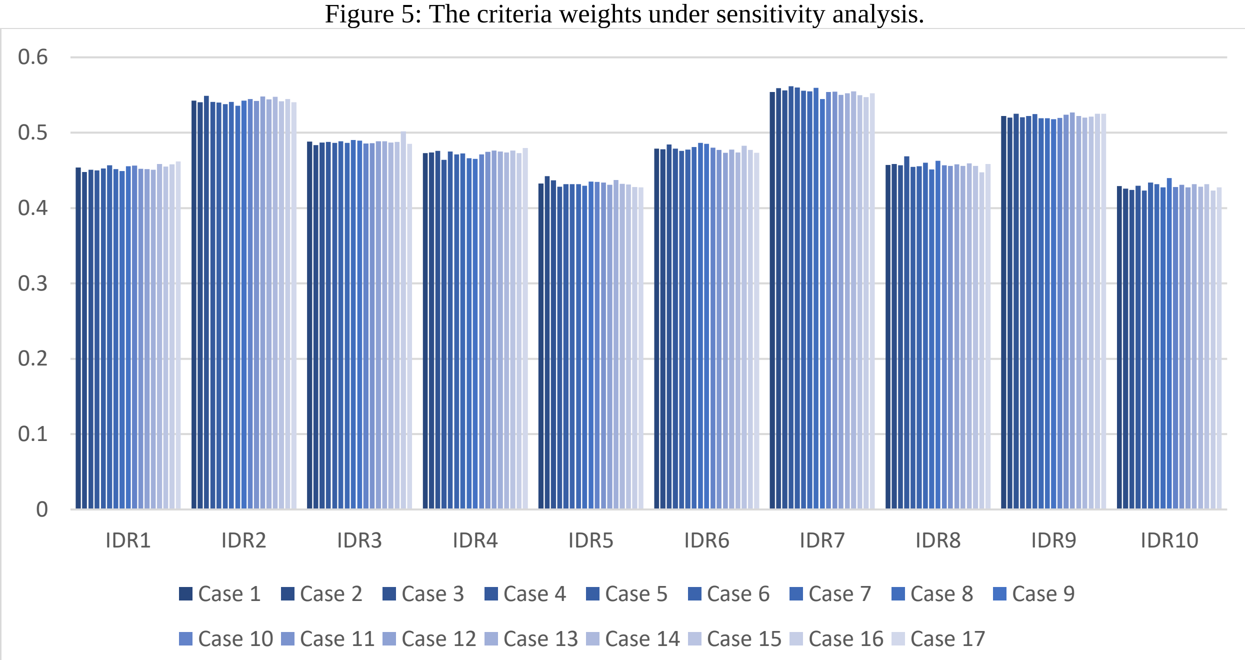

Figure 6: The closeness values under sensitivity analysis

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

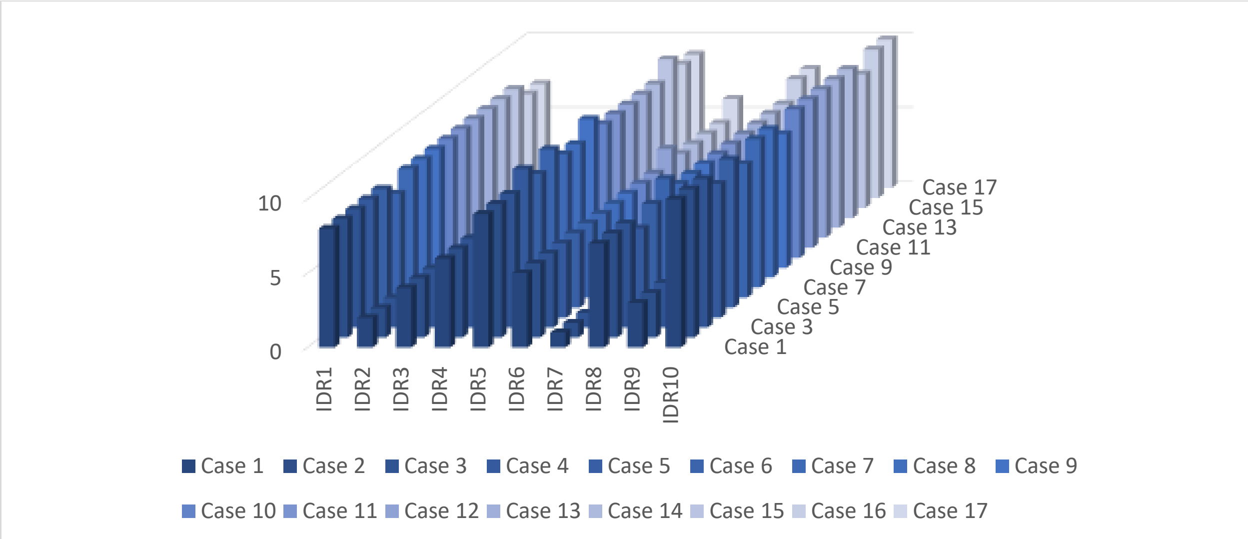

Figure 7: The rank of alternatives under sensitivity analysis.

5. Relative Analysis

This section shows the comparative analysis between the suggested method and other MCDM methods. The suggested method is compared with VIKOR, MABAC, and EDAS. Figure 8 shows the rank between the suggested method and other MCDM methods.

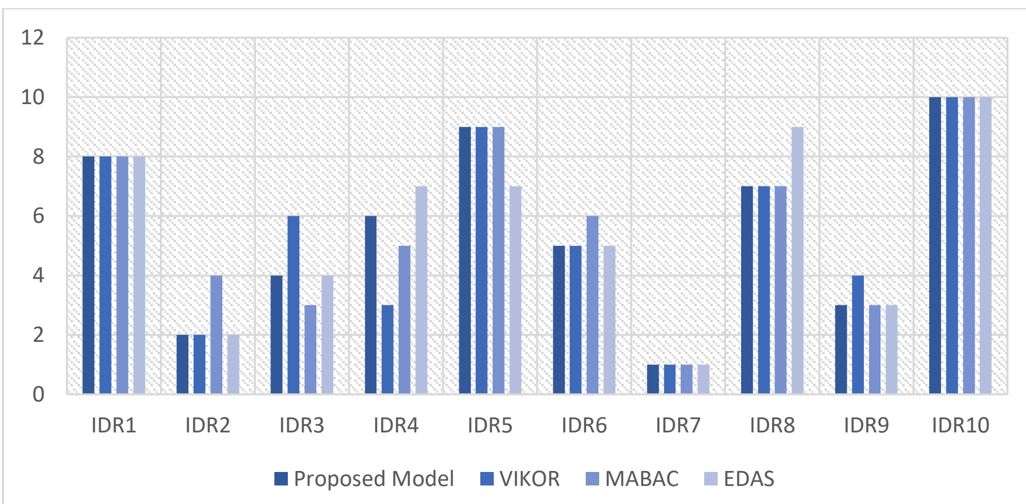

Figure 8: The rank of alternatives under comparative analysis.

6. Administrative Effects

This section can provide many benefits for managers who deal with intrusion detection responses by ranking the reaction in this paper as follows:

- Detects network-based assaults and outside hackers.
- Provides centralized administration to enable correlation of dispersed assaults.
- It allows the system administrator to measure the impact of assaults.
- Confers an extra degree of defense.
- Offers a comprehensive defense.
- Businesses may more easily comply with security laws by having more network visibility.

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

- Businesses may also use their IDS logs to demonstrate that they adhere to compliance obligations. Intrusion detection systems may also enhance security responses.

7. Conclusions

This study used the MCDM methodology for ranking intrusion response. The MCDM method is used under a single-valued neutrosophic set to deal with uncertainty. The TOPSIS method is an MCDM methodology used for ranking alternatives. This study used ten alternatives and 16 criteria. The experts evaluated the requirements and alternatives based on their opinions. Then, this study used the single-valued neutrosophic numbers to assess the requirements and alternatives. The criteria weights are computed to rank the priories in importance. Then, the TOPSIS method was applied to show the rank of other options. The rank of alternatives is calculated by using the closeness value. The sensitivity analysis was conducted in this study using seventeen cases. The criteria weights are changed under sensitivity analysis. Then, the closeness value is computed. The results show the rank of alternatives is stable under different cases. The suggested method was compared with other MCDM methods to show its effectiveness. The results show the suggested method is robust compared with other MCDM methods.

Acknowledgment

The authors are thankful to the Deanship of Graduate Studies and Scientific Research at the University of Bisha for supporting this work through the Fast-Track Research Support Program.

References

[1] H. Alyami *et al.*, "Effectiveness evaluation of different IDSs using integrated fuzzy MCDM model," *Electronics*, vol. 11, no. 6, p. 859, 2022.
[2] Y. B. Abushark *et al.*, "Cyber security analysis and evaluation for intrusion detection systems," *Comput. Mater. Contin*, vol. 72, pp. 1765–1783, 2022.
[3] M. A. Q. Martinez, D. T. L. Rugel, C. J. E. Alcivar, and M. Y. L. Vazquez, "A framework for selecting classification models in the intruder detection system using TOPSIS," in *Human Interaction, Emerging Technologies and Future Applications III: Proceedings of the 3rd International Conference on Human Interaction and Emerging Technologies: Future Applications (IHIET 2020), August 27-29, 2020, Paris, France*, Springer, 2021, pp. 173–179.
[4] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," *Cluster Computing*, vol. 26, no. 6, pp. 3753–3780, 2023.
[5] K. He, D. D. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2023.
[6] A. Alamleh *et al.*, "Multi-attribute decision-making for intrusion detection systems: A systematic review," *International Journal of Information Technology & Decision Making*, vol. 22, no. 01, pp. 589–636, 2023.
[7] A. Thakkar and R. Lohiya, "Fusion of statistical importance for feature selection in Deep Neural Network-based Intrusion Detection System," *Information Fusion*, vol. 90, pp. 353–363, 2023.
[8] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Cluster Computing*, vol. 26, no. 6, pp. 4069–4083, 2023.
[9] D. Karabašević *et al.*, "A novel extension of the TOPSIS method adapted for the use of single-valued neutrosophic sets and hamming distance for e-commerce development strategies selection," *Symmetry*, vol. 12, no. 8, p. 1263, 2020.
[10] Y. Sun and Y. Cai, "A flexible decision-making method for green supplier selection integrating TOPSIS and GRA under the single-valued neutrosophic environment," *IEEE Access*, vol. 9, pp. 83025–83040, 2021.
[11] Ş. Rıdvan, A. Fuat, and K. Gökçe Dilek, "A single-valued neutrosophic multicriteria group decision approach with DPL-TOPSIS method based on optimization," *International Journal of Intelligent Systems*, vol. 36, no. 7, pp. 3339–3366, 2021.
[12] A. Abdel-Monem, N. A. Nabeeh, and M. Abouhawwash, "An Integrated Neutrosophic Regional Management Ranking Method for Agricultural Water Management," *Neutrosophic Systems with Applications*, vol. 1, pp. 22–28, 2023.
[13] R. Mohamed and M. M. Ismail, "Harness Ambition of Soft Computing in Multi-Factors of Decision-Making Toward Sustainable Supply Chain in the Realm of Unpredictability," *Multicriteria Algorithms with Applications*, vol. 2, pp. 29–42, 2024.

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024

[14] S. Pramanik, P. P. Dey, and B. C. Giri, "TOPSIS for single valued neutrosophic soft expert set based multi-attribute decision-making problems," *Neutrosophic Sets and Systems*, vol. 10, pp. 88–95, 2015.

[15] J. Ye, "An extended TOPSIS method for multiple attribute group decision making based on single valued neutrosophic linguistic numbers," *Journal of Intelligent & Fuzzy Systems*, vol. 28, no. 1, pp. 247–255, 2015.

[16] P. Biswas, S. Pramanik, and B. C. Giri, "NonLinear programming approach for single-valued neutrosophic TOPSIS method," *New Mathematics and Natural Computation*, vol. 15, no. 02, pp. 307–326, 2019.

[17] Ş. Özlü and F. Karaaslan, "Hybrid similarity measures of single-valued neutrosophic type-2 fuzzy sets and their application to MCDM based on TOPSIS," *Soft Computing*, vol. 26, no. 9, pp. 4059–4080, 2022.

[18] K. M. Sallam and A. W. Mohamed, "Single Valued Neutrosophic Sets for Assessment Quality of Suppliers under Uncertainty Environment," *Multicriteria Algorithms with Applications*, vol. 1, no. 1, pp. 1–10, 2023.

[19] X. Peng and J. Dai, "Approaches to single-valued neutrosophic MADM based on MABAC, TOPSIS and new similarity measure with score function," *Neural Computing and Applications*, vol. 29, pp. 939–954, 2018.

[20] P. Biswas, S. Pramanik, and B. C. Giri, "TOPSIS method for multi-attribute group decision-making under single-valued neutrosophic environment," *Neural computing and Applications*, vol. 27, pp. 727–737, 2016.

[21] A. M. AbdelMouty and A. Abdel-Monem, "Neutrosophic MCDM Methodology for Assessment Risks of Cyber Security in Power Management," *Neutrosophic Systems with Applications*, vol. 3, pp. 53–61, 2023.

[22] Smarandache, F. (2019). Neutrosophic set is a generalization of intuitionistic fuzzy set, inconsistent intuitionistic fuzzy set (picture fuzzy set, ternary fuzzy set), pythagorean fuzzy set, spherical fuzzy set, and q-rung orthopair fuzzy set, while neutrosophication is a generalization of regret theory, grey system theory, and three-ways decision (revisited). Journal of New Theory, (29), 1-31.

[23] D. Liu and D. Xu, "A Novel TOPSIS Method for Multiple Attribute Decision Making Based on Single-Valued Neutrosophic Sets.," *IAENG International Journal of Applied Mathematics*, vol. 53, no. 1, 2023.

[24] S. S. Mohamed, A. Abdel-Monem, and A. A. Tantawy, "Neutrosophic MCDM Methodology for Risk Assessment of Autonomous Underwater Vehicles," *Neutrosophic Systems with Applications*, vol. 5, pp. 44–52, 2023.

[25] M. A. Talukder *et al.*, "A dependable hybrid machine learning model for network intrusion detection," *Journal of Information Security and Applications*, vol. 72, p. 103405, 2023.

[26] M. J. Idrissi *et al.*, "Fed-anids: Federated learning for anomaly-based network intrusion detection systems," *Expert Systems with Applications*, vol. 234, p. 121000, 2023.

[27] G. Logeswari, S. Bose, and T. Anitha, "An intrusion detection system for sdn using machine learning," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 867–880, 2023.

[28] S. Wang, W. Xu, and Y. Liu, "Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things," *Computer Networks*, vol. 235, p. 109982, 2023.

[29] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An effective intrusion detection approach based on ensemble learning for IIoT edge computing," *Journal of Computer Virology and Hacking Techniques*, vol. 19, no. 4, pp. 469–481, 2023.

[30] M. A. Hossain and M. S. Islam, "Ensuring network security with a robust intrusion detection system using ensemble-based machine learning," *Array*, vol. 19, p. 100306, 2023.

[31] H. Attou *et al.*, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing," *Applied Sciences*, vol. 13, no. 17, p. 9588, 2023.

[32] S. Venkatesan, "Design an intrusion detection system based on feature selection using ML algorithms," *Mathematical Statistician and Engineering Applications*, vol. 72, no. 1, pp. 702–710, 2023.

[33] S. Hariharan, R. R. Rejimol Robinson, R. R. Prasad, C. Thomas, and N. Balakrishnan, "XAI for intrusion detection system: comparing explanations based on global and local scope," *Journal of Computer Virology and Hacking Techniques*, vol. 19, no. 2, pp. 217–239, 2023.

[34] F. Karaaslan and F. Hunu, "Type-2 single-valued neutrosophic sets and their applications in multi-criteria group decision making based on TOPSIS method," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 4113–4132, 2020.

[35] A. Ashraf and M. A. Butt, "Extension of TOPSIS method under single-valued neutrosophic N-soft environment," *Neutrosophic sets and systems*, vol. 41, pp. 286–303, 2021.

[36] H. Garg, *Algorithms for single-valued neutrosophic decision making based on TOPSIS and clustering methods with new distance measure*. Infinite Study, 2020.

[37] J. Chen, S. Zeng, and C. Zhang, "An OWA distance-based, single-valued neutrosophic linguistic topsis approach for green supplier evaluation and selection in low-carbon supply chains," *International journal of environmental research and public health*, vol. 15, no. 7, p. 1439, 2018.

DOI: https://doi.org/10.54216/IJNS.230320
Received: July 12, 2023 Revised: November 15, 2023 Accepted: February 09, 2024