Integrated Neutrosophic methodology and Machine Learning Models for Cybersecurity Risk Assessment: An exploratory study

Ali Alqazzaz
Department of Information Systems and Cybersecurity, College of Computing and Information Technology, University of Bisha, P.O. Box 344, Bisha 61922, Saudi Arabia.
Email: aqzaz@ub.edu.sa

Abstract

Information technology security, or Cybersecurity, guards against hostile cyberattacks on computers, mobile devices, servers, electronic systems, and networks. Cybersecurity risks have been a significant concern for any vital digital infrastructure in recent years, and different online cyberattacks are also becoming a significant problem for society. Consequently, it's critical to adopt technology created to provide cybersecurity. However, one should consider the associated hazards while selecting among Cybersecurity systems. We have developed a multi-criteria decision-making (MCDM) approach based on a single-valued neutrosophic set (SVNS). This allows specialists more latitude in assessing the criteria and alternatives using language and overcoming uncertain information. The VIKOR is an MCDM methodology used to rank the other options. The VIKOR method is integrated with the neutrosophic set. There are 18 criteria, and 10 alternatives are used in this study. The sensitivity analysis and comparative analysis are conducted in this study. The sensitivity analysis results show the alternatives' rank is stable under different cases. The comparative analysis compares the suggested method with other MCDM methods. The comparative analysis shows the suggested method was effective compared with other MCDM methods. Machine learning methods predict the type of attack in Cybersecurity. This study uses Three machine learning methods: decision tree, random forest, and support vector machine.

Keywords: Cybersecurity; Risk Evaluation; SVNS; Machine Learning; Neutrosophic Set

1. Introduction

The fast advancement of technology and industry has made cybersecurity more critical. Several Cybersecurity issues have surfaced in this context due to technological advancements. About 40% of nations see cyberattacks as possible risks; therefore, as a consequence, global evaluation leads to the realization of Cybersecurity measures at all levels[1]–[3].

The increased interconnection of computers via the internet has made many online applications, including online banking, e-commerce, and m-commerce, vulnerable to cyberattacks. Aside from its many benefits, the expanding digital world poses severe risks to a nation's defense sector and other vital government agencies. Because of the rise in cybercrimes, cybersecurity is becoming a significant global idea. Cyberattack losses have made it imperative for information security pioneers to build trustworthy and robust safeguards[4]–[7].

Since the phrase "Cybersecurity" is so broad, a few distinct definitions exist in the literature. The assets of an organization or user are comprised of individuals, connected computer devices, infrastructure, applications, services, communications networks, and information in the digital space[8]–[10].

Cybersecurity measures aim to defend against security threats in the cyber environment by maintaining and perceiving security features. Cybersecurity is the prevention of attacks, unauthorized access, alteration, or destruction of computers, networks, programs, and data by a collection of technologies and procedures. Network and software security systems are included in Cybersecurity structures, and they all need to include firewalls, antivirus programs, and intrusion detection systems (IDS). Information system unauthorized use, duplication, change, and destruction may

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

all be detected and identified using IDSs. The assaults on the organization, both internal and external, constitute security violations[5], [10].

Information security dramatically depends on the use of cybersecurity technology. There are a lot of Cybersecurity technologies in the literature. Companies will gain significantly by prioritizing these technologies and evaluating if they are essential. But it's also important to consider the threats these technologies pose[11], [12].

This paper used multi-criteria decision-making (MCDM) [13], [14]for the evaluation of risks of Cybersecurity under a neutrosophic set. The neutrosophic set [15] is used to overcome uncertain information[16], [17]. Then, the machine learning methods are used to predict the outcome of the type of attack and risk.

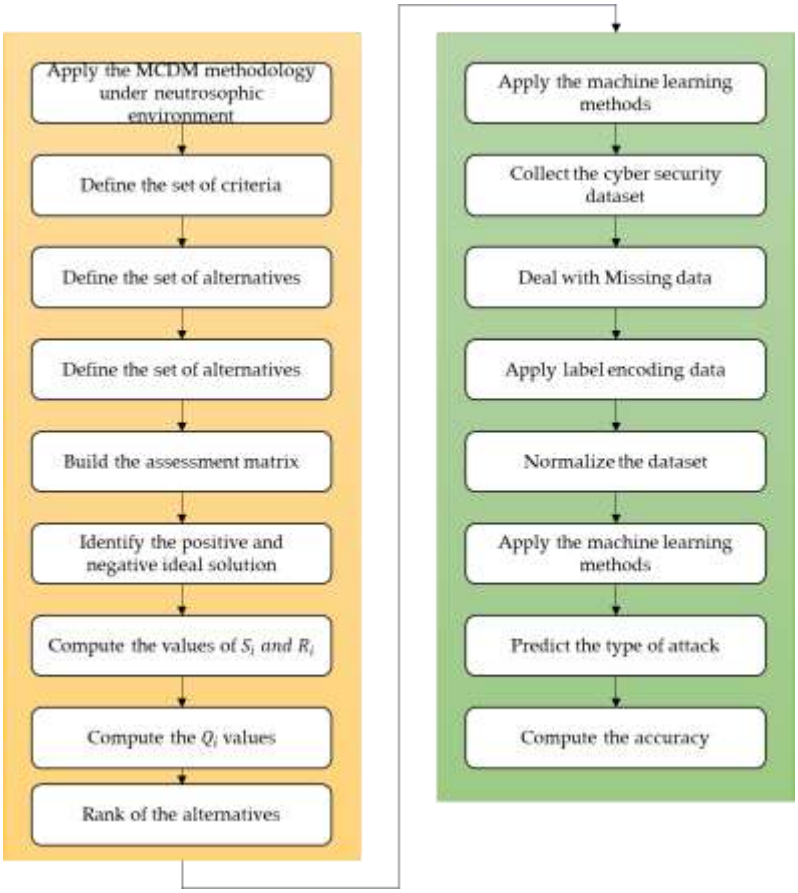

Figure 1: The steps of the suggested methodology.

2. Materials and Methods

This section introduces two parts, in the first part, the VIKOR method is introduced under a neutrosophic set to overcome the uncertainty information[18], [19]. In the second part, machine learning methods are introduced to show the type of attack in Cybersecurity[20]–[22]. Figure 1 shows the research framework.

The neutrosophic set is a branch of neutrosophy that studies the nature, scope, and genesis of neutralities as well as how they interact with various ideational frameworks. It is a strong general formal framework that expands on the sets that are offered from a philosophical perspective. The following is definition of a neutrosophic set[23]:

Definition 1[23]

Let X be a universe of discourse and $T_Y(x), I_Y(x), and\ F_Y(x)$ refer to the truth, indeterminacy and falsity membership degrees. Where $T_Y(x) \rightarrow]0-,1+[, I_Y(x) \rightarrow]0-,1+[, F_Y(x) \rightarrow]0-,1+[$

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

$0-\leq sup\ T_Y(x) + sup\ T_Y(x) + sup\ T_Y(x) \leq 3+$

Definition 2:

Single valued neutrosophic set can be defined as:

$N = \{< x, T_N(x), I_N(x), F_N(x) > \mid x \in X\}$

Definition 3

Let $a = (T_a, I_a, F_a)\ and\ b = (T_b, I_b, F_b)$ be two single valued neutrosophic numbers, then their operations can be defined as

$a^c = (F_a, 1 - I_a, T_a)$

$a \cup b = \left(\max\{T_a, T_y\}, \min\{I_a, I_y\}, \min\{F_a, F_y\}\right)$

$a \cap b = \left(\min\{T_a, T_y\}, \max\{I_a, I_y\}, \max\{F_a, F_y\}\right)$

$a \oplus b = (T_a + T_b - T_a * T_b, I_a * I_b, F_a * F_b)$

$a \otimes b = (T_a * T_b, I_a + I_b - F_a * F_b, F_a + F_b - F_a * F_b)$

$\wedge a = (1 - (1 - T_a)^\wedge, (I_a)^\wedge, (F_a)^\wedge)$

$a^\wedge = ((T_a)^\wedge, 1 - (1 - I_a)^\wedge, 1 - (1 - F_a)^\wedge)$

Definition 4

The score function of single valued neutrosophic numbers is:

$S(a) = \frac{2+T_a-I_a-F_a}{3}$

Definition 5

The single valued neutrosophic weighted averaging operator can be computed as:

$WA(a_1, a_2, \dots a_n) = \left(1 - \prod_{j=1}^{n}(1 - T_j)^{w_j}, \prod_{j=1}^{n}(I_j)^{w_j}, \prod_{j=1}^{n}(F_j)^{w_j}\right)$

Definition 6

The single valued neutrosophic weighted geometric operator can be computed as:

$WG(a_1, a_2, \dots a_n) = \left(\prod_{j=1}^{n}(T_j)^{w_j}, 1 - \prod_{j=1}^{n}(1 - I_j)^{w_j}, 1 - \prod_{j=1}^{n}(1 - F_j)^{w_j}\right)$

Definition 7

The cosine similarity degree as:

$C(a) = \frac{T_a}{\sqrt{T_a^2 + I_a^2 + F_a^2}}$

The VIKOR method is used under a neutrosophic set to rank the alternatives. The steps of the VIKOR method are discussed as follows:

Step 1. Build the assessment matrix

$$X = \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix} \quad (1)$$

Where m refers to the number of alternatives and n refers to the number of criteria.

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

Step 2. Identify the positive and negative ideal solution

$$x_j^+ = \max(x_{ij}) \tag{2}$$

$$x_j^- = \min(x_{ij}) \tag{3}$$

Step 3. Compute the values of S_i and R_i

$$S_i = \sum_{j=1}^{n} w_j(x_j^+ - x_{ij}) \,/\, (x_j^+ - x_j^-) \tag{4}$$

$$R_i = \max_j \{w_j(x_j^+ - x_{ij})/(x_j^+ - x_j^-)\} \tag{5}$$

Step 4. Compute the Q_i values

$$Q_i = \delta\left(\frac{S_i - \min S_i}{(\max S_i - \min S_i)}\right) + (1-\delta)\left(\frac{R_i - \min R_i}{(\max R_i - \min R_i)}\right) \tag{6}$$

Where $\delta \in [0,1]$

2.1 Machine learning

A subfield of artificial intelligence called "machine learning" seeks to allow computers to learn how to carry out specific tasks without human programming. The foundation of this method is the creation of models that, given fresh data, may be used to learn from the data and make predictions or judgments. Deep Learning (DL) is an advancement in machine learning (ML) that makes use of an Artificial Neural Network (ANN), which is a multi-layered structure. Less human intervention is needed with DL algorithms since features are automatically extracted. However, DL differs significantly from other ML approaches in that it needs a large amount of data to function successfully[24]–[26].

While machine learning (ML) and deep learning (DL) are relatively new ideas, the first computer learning program was created in 1952 by Arthur Samuel and the first neural network was suggested in 1957 by Frank Rosenblatt. Both machine and deep learning have advanced significantly during the 1990s, mainly due to increased processing power and the availability of vast volumes of data. Numerous machine-learning techniques are available that may be used to address various issues. We will only examine algorithms used for pollutant measure prediction in this section[27], [28].

Although it may also be used to solve regression issues, the k-nearest neighbors approach is often used to solve classification difficulties. This algorithm's concept is straightforward. The method determines the distance between an information point and the training dataset points to choose the k closest ones and construct their average as forecasting, given a distance (Euclidean distance, Mahalanobis distance, etc.) and a k value. The weighted k-nearest-neighbors (WKNN) method is an enhancement of this approach. In this instance, the prediction's computation considers a weighted arithmetic mean[29], [30].

The creation of multiple decision trees serves as the foundation for Random Forest. The forecast will be the mean of the estimates made by the various trees. Each decision tree is built using a sample of data from the training dataset. The decision tree error will be estimated using the remaining data. Random selection determines the subset of independent factors that may divide each node[31], [32].

Creating a model for forecasting a quantitative variable from a group of independent factors is the goal of this approach. The recursive partitioning is the foundation of the method. Decision nodes and leaves make up trees. When constructing DT regression, the standard deviation reduction is often considered to decide how to divide a node into two or more branches. The root node is the first decision node to be split based on the most significant independent variable. The variable with the lowest sum of the squared estimate of errors (SSE) is taken into consideration as the decision node, and nodes are separated once more. The values of the chosen variable are used to partition the dataset. When a predetermined termination condition is met, the process is said to have ended[33], [34].

3. Results

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

In the first part, the neutrosophic VIKOR method is introduced to rank the alternatives. This study used 18 criteria and 10 alternatives. The criteria of this study are shown in Figure 2. This study used a single valued neutrosophic scale [35]as shown in below table

Linguistic Variables	Single valued neutrosophic numbers
Extremely significant	(0.9,0.1,0.1)
Very High significant	(0.8,0.20,0.15)
High significant	(0.7, 0.3, 0.2)
Significant	(0.6, 0.4, 0.3)
Significant Equal	(0.5, 0.5, 0.5)
insignificant	(0.6, 0.6, 0.55)
low insignificant	(0.4, 0.7, 0.6)
Very Low insignificant	(0.3, 0.8, 0.7)
Very very low insignificant	(0.2, 0.9, 0.8)
Extremely insignificant	(0.1, 0.95, 0.85)

Figure 2: Risk criteria of Cybersecurity.

Step 1. Build the assessment matrix by using Eq. (1). Then compute the criteria weights as shown in Figure 3.

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

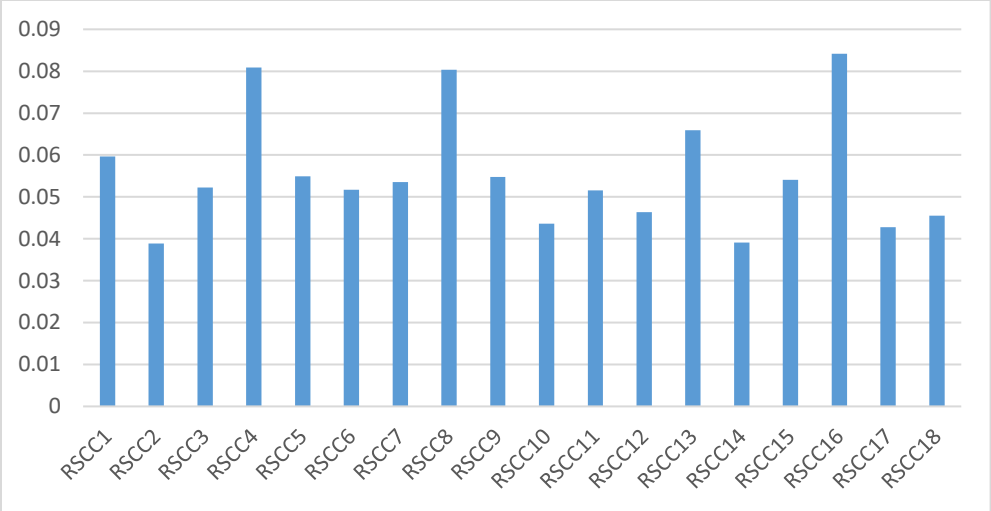

Figure 3: The weights of risks Cybersecurity criteria.

Step 2. Identify the positive and negative ideal solution by using Eqs. (2 and 3).

Step 3. Compute the values of S_i *and* R_i by using Eqs. (4 and 5) as shown in Table 1.

Table 1: The normalization decision matrix.

	$RSCC_1$	$RSCC_2$	$RSCC_3$	$RSCC_4$	$RSCC_5$	$RSCC_6$	$RSCC_7$	$RSCC_8$	$RSCC_9$	$RSCC_{10}$	$RSCC_{11}$	$RSCC_{12}$	$RSCC_{13}$	$RSCC_{14}$	$RSCC_{15}$	$RSCC_{16}$	$RSCC_{17}$	$RSCC_{18}$
$RSCA_1$	0.053766	0.035584	0.027804	0.010475	0.034564	0	0.037251	0.002146	0.034322	0.036588	0.051563	0.046319	0.035042	0.021433	0.025171	0	0.026464	0.021879
$RSCA_2$	0	0.023671	0.026593	0.037846	0.021612	0.051726	0.025701	0.04924	0.02146	0.039342	0.051563	0.040629	0.03511	0.037138	0.023416	0.002465	0.026464	0.04555
$RSCA_3$	0.025076	0.031768	0.027804	0	0.039835	0.043993	0.033725	0.001824	0.039855	0.02004	0.051563	0.00693	0.00153	0.01047	0.045994	0.040782	0.04274	0.028215
$RSCA_4$	0.040764	0.023671	0.027804	0.068258	0.054896	0.037427	0.001469	0.080351	0.034322	0.033133	0	0.046351	0.065937	0.039113	0.041951	0.084141	0.026464	0.001973

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

$RSCA_5$	$RSCA_6$	$RSCA_7$	$RSCA_8$	$RSCA_9$	$RSCA_{10}$
0.032378	0.012981	0.032378	0.032311	0.053766	0.059667
0	0.023671	0.018205	0.012377	0.014801	0.038885
0	0.027804	0.027786	0	0.027804	0.052216
0.072313	0.080873	0.030412	0.049786	0.06792	0.062288
0.054896	0.042923	0.026582	0.054369	0	0.026582
0.000146	0.024295	0.01605	0.024295	0.016007	0.007952
0.053563	0	0	0.001411	0.025716	0.025936
0.066512	0.04924	0.070696	0.025747	0	0.04924
0.054765	0.026396	0.034322	0.001271	0.034322	0
0.043583	0.026986	0.033809	0.026986	0	0.02047
0.031361	0.051457	0	0.039465	0.025488	0.051563
0.027912	0.046351	0.00693	0.027912	0.038149	0
0.001683	0.047655	0.027002	0.021954	0	0.03511
0.010766	0.039113	0.01047	0.01047	0	0.039113
0.054079	0.025171	0	0	0.038824	0.054079
0.002465	0.05165	0.01266	0.033836	0.05165	0.000224
0	0.028695	0.020074	0.00639	0.016095	0.026464
0.03485	0.028215	0.021879	0	0.021699	0.021879

Step 4. Compute the Q_i values by using Eq. (6) as shown in Figure 4.

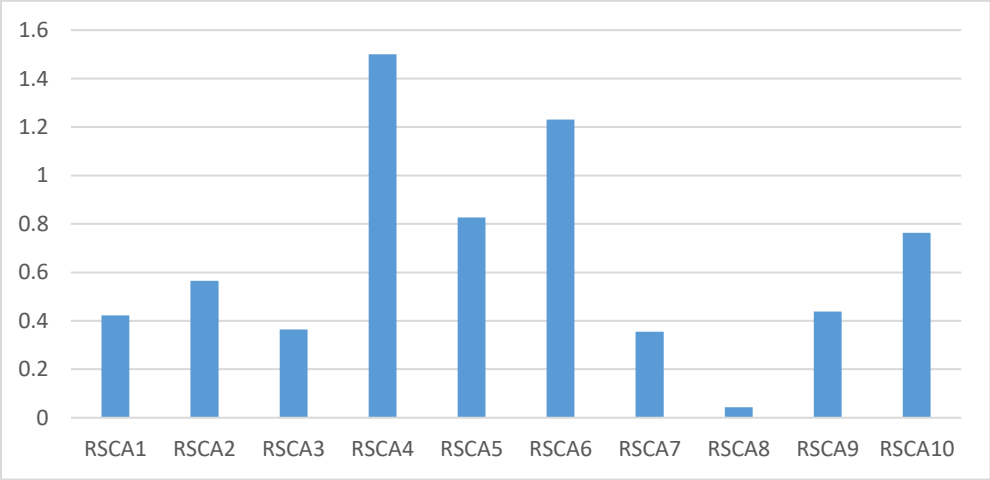

Figure 4: The values of Q_i.

3.1 Machine Learning Results

The scikit-learn package's algorithms offer a binary or multiclass categorization. For this tool to be used properly, choosing the suitable model is crucial, as is determining which sort of algorithm—supervised or unsupervised—will best solve the issue. Next, a subset of variables is selected to train these models without making hyperparameter adjustments. This process often results in a reduction in training time and the best metric. In this situation, performance

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

measurements are crucial for several modeling processes, including choosing the model type, assessing the finished product, and monitoring[36]–[38]. The accessible metrics that assess a classification model's performance are the F1 score, accuracy, precision, and recall. These metrics are specified by

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (7)$$

$$Precision = \frac{TP}{TP + FP} \quad (8)$$

$$Recall = \frac{TP}{TP + FN} \quad (9)$$

$$F_1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (10)$$

The dataset from Kaggle has 40000 rows and 25 columns used for prediction type of attack in this study. Two columns in the dataset have the 20000 rows missing values. Then, we drop these columns to delete all missing values. Table 2 shows the head of the used dataset.

Table 2: The head of the used dataset.

	0	1	2	3	4
Timestamp	5/30/2023 6:33	8/26/2020 7:08	11/13/2022 8:23	7/2/2023 10:38	7/16/2023 13:11
Source IP Address	103.216.15.12	78.199.217.198	63.79.210.48	163.42.196.10	71.166.185.76
Destination IP Address	84.9.164.252	66.191.137.154	198.219.82.17	101.228.192.255	189.243.174.238
Source Port	31225	17245	16811	20018	6131
Destination Port	17616	48166	53600	32534	26646
Protocol	ICMP	ICMP	UDP	UDP	TCP
Packet Length	503	1174	306	385	1462
Packet Type	Data	Data	Control	Data	Data
Traffic Type	HTTP	HTTP	HTTP	HTTP	DNS
Payload Data	Qui natus odio asperiores nam. Optio nobis ius...	Aperiam quos modi officiis veritatis rem. Omni...	Perferendis sapiente vitae soluta. Hic delectu...	Totam maxime beatae expedita explicabo porro l...	Odit nesciunt dolorem nisi iste iusto. Animi v...
Anomaly Scores	28.67	51.5	87.42	15.79	0.52
Attack Type	Malware	Malware	DDoS	Malware	DDoS
Attack Signature	Known Pattern B	Known Pattern A	Known Pattern B	Known Pattern B	Known Pattern B
Action Taken	Logged	Blocked	Ignored	Blocked	Blocked
Severity Level	Low	Low	Low	Medium	Low
User Information	Reyansh Dugal	Summer Rana	Himmat Karpe	Fateh Kibe	Dhanush Chad
Device Information	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT ...	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT ...	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT ...	Mozilla/5.0 (Macintosh; PPC Mac OS X 10_11_5; ...	Mozilla/5.0 (compatible; MSIE 5.0; Windows NT ...
Network Segment	Segment A	Segment B	Segment C	Segment B	Segment C
Geo-location Data	Jamshedpur, Sikkim	Bilaspur, Nagaland	Bokaro, Rajasthan	Jaunpur, Rajasthan	Anantapur, Tripura
Log Source	Server	Firewall	Firewall	Firewall	Firewall

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

Figure 5 shows the number of attack types on the dataset used. The dataset has three types of attack: DDOS, malware, and intrusion. The DDOS has 13428 rows, the malware has 13307a rows, and intrusion has 13265 rows. The biggest number of rows is DDOS, followed by intrusion and malware.

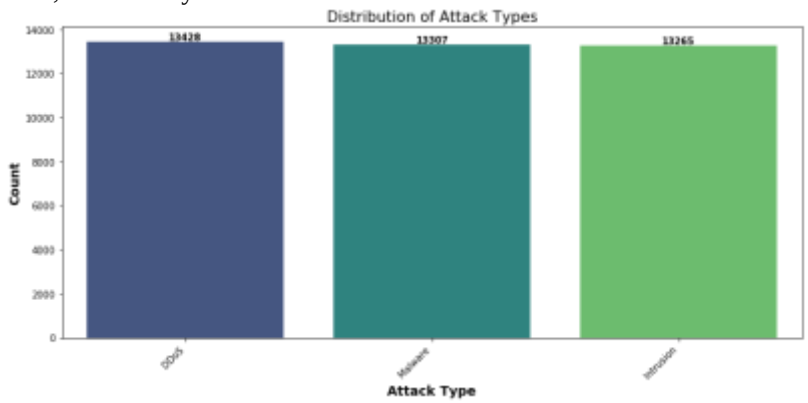

Figure 5: The types of attacks.

Figures 6, 7, and 8 show the distribution between attack type and anomaly score, source port, and packet length. These figures show the boxplot graph. The distribution shows the number of packet lengths between three types of attack.

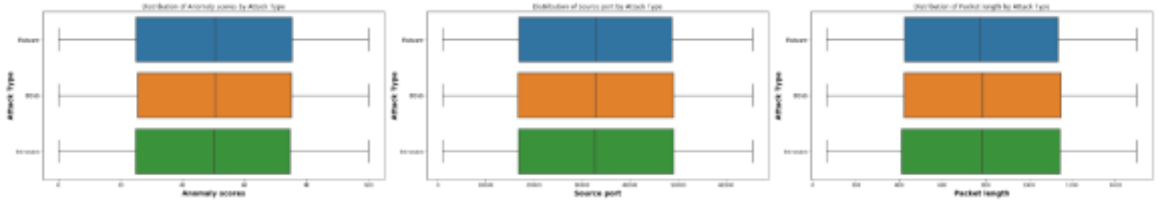

Figure 6: The distribution between attack type and anomaly score. Figure 7: The distribution between attack type and source port. Figure 8: The distribution between attack type and packet length.

Figure 9 shows the distribution network traffic protocol, including three protocols: UDP, TCP, and ICMP. The UDP has 33.6% of network traffic, TCP has 33.2%, and ICMP has 33.2% of network traffic.

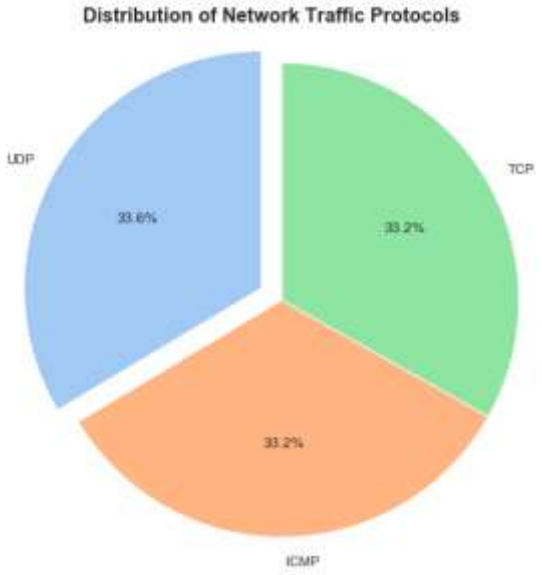

Figure 9: The distribution of network traffic protocol.

Figures 10 and 11 show the heatmap between years and months and month and weekday. The heatmap shows the relations between the criteria of the dataset.

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

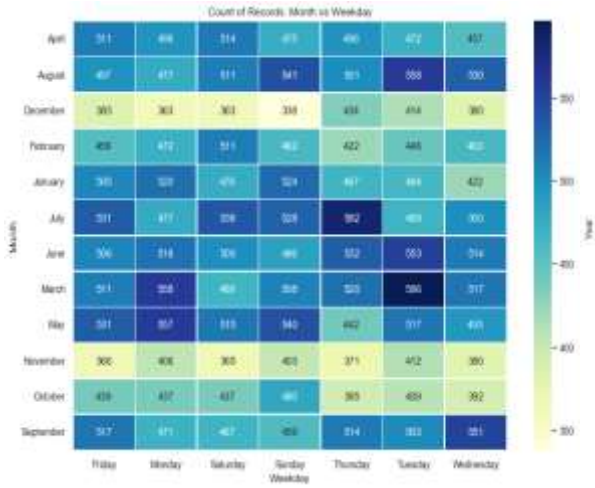

Figure 10: Heatmap between month and weekday.

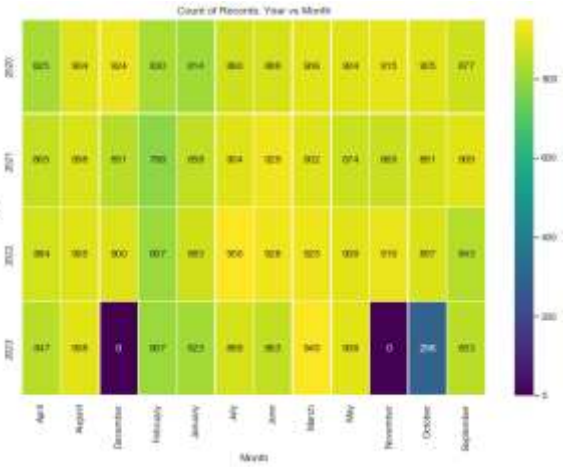

Figure 11: Heatmap between year and month.

Then, we applied the machine learning algorithms to show the prediction type of attack. The random forest has the highest accuracy, followed by the decision tree and support vector machine methods.

4. Analysis

This section introduces two parts; in the first part, the sensitivity analysis is introduced to show the results' stability. In the second part, the comparative analysis is introduced to show the effectiveness of the neutrosophic framework.

4.1 Sensitivity Analysis

This section introduces the sensitivity analysis to show the stability of the rank of alternatives. This study changes the VIKOR parameter value between 0 and 1. Then compute the rank of alternatives under the neutrosophic set. The values of Q_i are computed and shown in Figure 12. The ranking of the alternatives is shown in Figure 13. The results show the rank of alternatives is stable. The all cases show that alternative 4 is the worst. Only cases 1,2 show that alternative 3 is the best and in all other cases alternative 8 is the best.

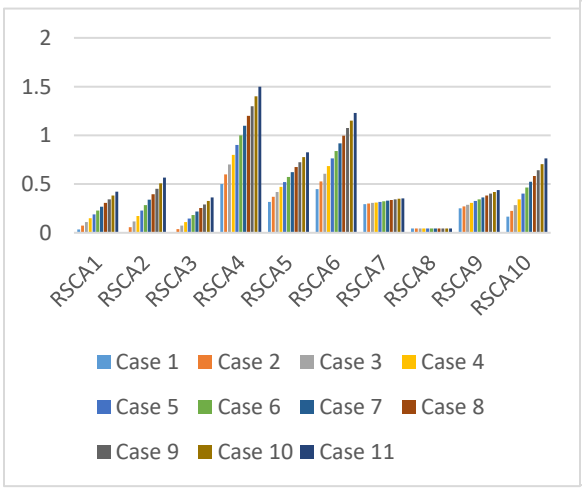

Figure 12: The values of Q_i under sensitivity analysis.

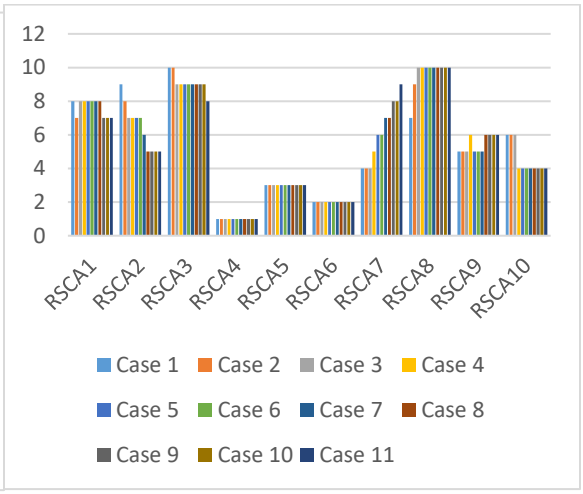

Figure 13: The rank of alternatives under sensitivity analysis.

4.2 Comparative Analysis

This part compares other MCDM methods, such as TOPSIS, EDAS, and MABAC. The results show that all methods show that alternative 8 is the best and alternative 3 is the worst. Figure 14 shows the comparative analysis.

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

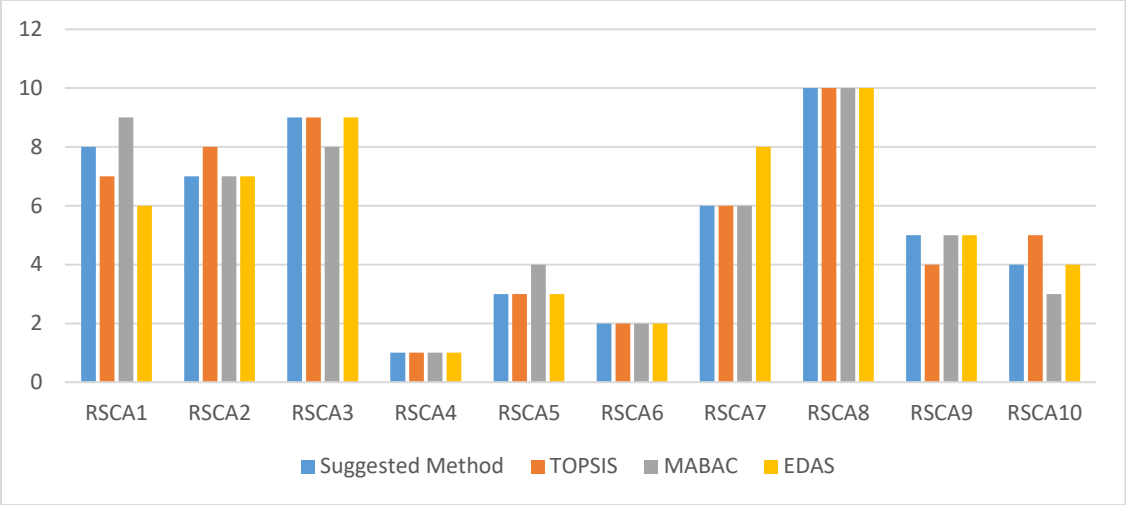

Figure 14: The comparison between the suggested method and other MCDM methods.

5. Conclusions

Technologies related to Cybersecurity are crucial instruments for defending networks against online threats. Nevertheless, by keeping an eye on networks and computer devices, these technologies compromise people's privacy. As such, businesses must consider these risks when selecting cybersecurity systems. We undertake research that considers the hazards to evaluate the significance of Cybersecurity technologies in this article. We use an MCDM technique to rank alternatives since the decision-making process involves several assessment criteria and alternatives—the MCDM methodology used with the neutrosophic set to overcome uncertainty in the evaluation process. The VIKOR method is used to rank the other options. The 18 criteria and 10 alternatives are used in this paper. Experts and decision-makers used the neutrosophic numbers to evaluate the requirements and alternatives. The sensitivity analysis is used to show the stability of the results. The sensitivity analysis was conducted by changing the VIKOR parameter to show the rank of alternatives under different cases. The results show the rank of alternatives is stable. The comparative analysis compared the suggested method with other MCDM methods. The results show the suggested method is effective compared with other MCDM methods. The machine learning algorithms are applied in this study to predict the type of attack. The random forest has the highest accuracy.

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] S. Musman and A. Turner, "A game theoretic approach to cyber security risk management," *The Journal of Defense Modeling and Simulation*, vol. 15, no. 2, pp. 127–146, 2018.

[2] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Computers & security*, vol. 56, pp. 1–27, 2016.

[3] J. J. Cebula and L. R. Young, "A taxonomy of operational cyber security risks," *Software Engineering Institute, Carnegie Mellon University*, 2010.

[4] H. I. Kure, S. Islam, and M. A. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Applied Sciences*, vol. 8, no. 6, p. 898, 2018.

[5] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA transactions*, vol. 46, no. 4, pp. 583–594, 2007.

[6] C. Florackis, C. Louca, R. Michaely, and M. Weber, "Cybersecurity risk," *The Review of Financial Studies*, vol. 36, no. 1, pp. 351–407, 2023.

[7] P. Katsumata, J. Hemenway, and W. Gavins, "Cybersecurity risk management," in *2010-MILCOM 2010 Military Communications Conference*, IEEE, 2010, pp. 890–895.

[8] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, "Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation," *Risk Analysis*, vol. 42, no. 8, pp. 1643–1669, 2022.

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

[9] D. W. Hubbard and R. Seiersen, *How to measure anything in cybersecurity risk*. John Wiley & Sons, 2023.
[10] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," *Computers & security*, vol. 31, no. 4, pp. 597–611, 2012.
[11] L. Allodi and F. Massacci, "Security events and vulnerability data for cybersecurity risk estimation," *Risk Analysis*, vol. 37, no. 8, pp. 1606–1627, 2017.
[12] S. L. Garfinkel, "The cybersecurity risk," *Communications of the ACM*, vol. 55, no. 6, pp. 29–32, 2012.
[13] A. El-Douh, S. Lu, A. Abdelhafeez, and A. Aziz, "A Neutrosophic Multi-Criteria Model for Evaluating Sustainable Soil Enhancement Methods and their Cost 2 Implications in Construction," *SMIJ*, vol. 5, no. 2, p. 11, 2023.
[14] 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.
[15] A. H. Abdel-aziem, H. K. Mohamed, and A. Abdelhafeez, "Neutrosophic Decision Making Model for Investment Portfolios Selection and Optimizing based on Wide Variety of Investment Opportunities and Many Criteria in Market," *Neutrosophic Systems with Applications*, vol. 6, pp. 32–38, 2023.
[16] S. Manna, T. M. Basu, and S. K. Mondal, "A soft set based VIKOR approach for some decision-making problems under complex neutrosophic environment," *Engineering Applications of Artificial Intelligence*, vol. 89, p. 103432, 2020.
[17] M. Abdel-Baset, V. Chang, A. Gamal, and F. Smarandache, "An integrated neutrosophic ANP and VIKOR method for achieving sustainable supplier selection: A case study in importing field," *Computers in Industry*, vol. 106, pp. 94–110, 2019.
[18] A. Abdelhafeez, H. Mahmoud, and A. S. Aziz, "Identify the most Productive Crop to Encourage Sustainable Farming Methods in Smart Farming using Neutrosophic Environment," *Neutrosophic Systems with Applications*, vol. 6, pp. 17–24, 2023.
[19] 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.
[20] M. Abdel-Basset, Y. Zhou, M. Mohamed, and V. Chang, "A group decision making framework based on neutrosophic VIKOR approach for e-government website evaluation," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 6, pp. 4213–4224, 2018.
[21] H. Eroğlu and R. Şahin, "A neutrosophic VIKOR method-based decision-making with an improved distance measure and score function: case study of selection for renewable energy alternatives," *Cognitive Computation*, vol. 12, no. 6, pp. 1338–1355, 2020.
[22] X. Luo, Z. Wang, L. Yang, L. Lu, and S. Hu, "Sustainable supplier selection based on VIKOR with single-valued neutrosophic sets," *Plos one*, vol. 18, no. 9, p. e0290093, 2023.
[23] 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.
[24] S. Yassine and A. Stanulov, "A comparative analysis of machine learning algorithms for the purpose of predicting Norwegian air passenger traffic," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, pp. 28–43, 2024.
[25] A. Singh, N. Thakur, and A. Sharma, "A review of supervised machine learning algorithms," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, Ieee, 2016, pp. 1310–1315.
[26] S. K. Parhi and S. K. Panigrahi, "Alkali–silica reaction expansion prediction in concrete using hybrid metaheuristic optimized machine learning algorithms," *Asian Journal of Civil Engineering*, vol. 25, no. 1, pp. 1091–1113, 2024.
[27] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN computer science*, vol. 2, no. 3, p. 160, 2021.
[28] L. Zheng, M. Mueller, C. Luo, and X. Yan, "Predicting whole-life carbon emissions for buildings using different machine learning algorithms: A case study on typical residential properties in Cornwall, UK," *Applied Energy*, vol. 357, p. 122472, 2024.
[29] B. J. Chelliah, T. P. Latchoumi, and A. Senthilselvi, "Analysis of demand forecasting of agriculture using machine learning algorithm," *Environment, Development and Sustainability*, vol. 26, no. 1, pp. 1731–1747, 2024.
[30] L. Lewis, H.-Y. Huang, V. T. Tran, S. Lehner, R. Kueng, and J. Preskill, "Improved machine learning algorithm for predicting ground state properties," *Nature Communications*, vol. 15, no. 1, p. 895, 2024.
[31] Z. Zhang, C. Johansson, M. Engardt, M. Stafoggia, and X. Ma, "Improving 3-day deterministic air pollution

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024

forecasts using machine learning algorithms," *Atmospheric Chemistry and Physics*, vol. 24, no. 2, pp. 807–851, 2024.
[32] M. Khan *et al.*, "Intelligent prediction modeling for flexural capacity of FRP-strengthened reinforced concrete beams using machine learning algorithms," *Heliyon*, vol. 10, no. 1, 2024.
[33] G. Bonaccorso, *Machine learning algorithms*. Packt Publishing Ltd, 2017.
[34] B. Mahesh, "Machine learning algorithms-a review," *International Journal of Science and Research (IJSR).[Internet]*, vol. 9, pp. 381–386, 2020.
[35] R. Sundareswaran *et al.*, "Assessment of structural cracks in buildings using single-valued neutrosophic DEMATEL model," *Materials Today: Proceedings*, vol. 65, pp. 1078–1085, 2022.
[36] M. Alyami *et al.*, "Predictive modeling for compressive strength of 3D printed fiber-reinforced concrete using machine learning algorithms," *Case Studies in Construction Materials*, vol. 20, p. e02728, 2024.
[37] D. Hu, Y. Wang, G. Ji, and Y. Liu, "Using machine learning algorithms to predict the prognosis of advanced nasopharyngeal carcinoma after intensity-modulated radiotherapy," *Current Problems in Cancer*, vol. 48, p. 101040, 2024.
[38] A. Borodulin, A. Gladkov, A. Gantimurov, V. Kukartsev, and D. Evsyukov, "Using machine learning algorithms to solve data classification problems using multi-attribute dataset," in *BIO Web of Conferences*, EDP Sciences, 2024, p. 2001.

Doi: https://doi.org/10.54216/IJNS.230317
Received: August 16, 2023 Revised: November 22, 2023 Accepted: January 30, 2024