NSS
Neutrosophic Sets and Systems, Vol. 83, 2025
University of New Mexico

Machine Learning Models with Neutrosophic Numbers for Network Anomaly Detection and Security Defense Technology

Hussein S Al-Khazraji[1], Ahmed M. Alkhamees[2], Humam M Al-Doori[3], Ahmed A. Metwaly[4], Mohamed eassa[5,6], Ahmed Abdelhafeez[5,6], Ahmed S. Salama[7], Ahmad M. Nagm[7]

[1]Department of Electrical Power Engineering Technologies, Al-Hussein University College, Karbala, Iraq

hussain.safaa@huciraq.edu.iq

[2]College of Health and Medical Technologies / Department of Anesthesia Technologies, Ahl Al Bayt University

Karbala, Iraq, Iraq, Ahmedmon89@abu.edu.iq

[3]Department of Computer Engineering Techniques, Al-Yarmok University College,Diyala, Iraq,

[4]Department of Computer Science, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt, a.metwaly23@fci.zu.edu.eg

[5]Computer Science Department, Faculty of Information Systems and Computer Science, October 6 University, Giza, 12585, Egypt mohamed.eassa.cs@o6u.edu.eg; aahafeez.scis@o6u.edu.eg
[6]Applied Science Research Center. Applied Science Private University, Amman, Jordan
[7]Department of Computer Engineering and Electronics, Cairo Higher Institute for Engineering, Computer Science and Management, New Cairo, Egypt ahmadnagm@alazhar.edu.eg, A.salama@chi.edu.eg

Abstract: In the dynamic world of cybersecurity, strong solutions are necessary to safeguard intricate network systems. By looking at network anomaly detection and security protection, this study investigates how machine learning (ML) might increase digital infrastructure security. We assess how well critical ML approaches, such as ensemble approaches and supervised learning, identify anomalies and lessen risks. The examination of ML-based systems integration into comprehensive security frameworks places a strong emphasis on real-time monitoring and adaptive responses. Examples from real-world situations highlight how crucial ML is to improving network security. After, we apply different ML models to the real-world dataset. Then we use the single-valued Neutrosophic numbers (SVNNs) methodology to evaluate these ML models and select the best one. We use the multi-criteria decision-making (MCDM) approach to obtain the criteria weights and rank the ML models using the EDAS method. The results show that the random forest model is the best ML model under different evaluation matrices.

Keywords: Neutrosophic Number; Security; Network Anomaly Detection; Cybersecurity; Uncertainty.

1. Introduction

Network security is a crucial concern in today's technologically advanced society because of the ever-changing cyber threats. Which pose serious difficulties for both people and organizations.[1]. The interconnectedness of digital ecological systems, which include personal gadgets and critical infrastructure, exacerbates the impact of intrusions. The main topic of this paper is the complexity and urgency of network security, which emphasizes the use of machine learning (ML) in identifying network abnormalities and defending against them.[2].

Machine learning (ML) has been shown to be a powerful tool in cybersecurity, successfully managing the complexity and dynamic nature of cyber threats. Through trend identification and prediction analysis, machine learning (ML) enables initiative-taking threat detection and real-time monitoring, in contrast to traditional security methods. Because of its ability to continually adapt from fresh data, it efficiently counters sophisticated attacks that often evade traditional defenses.[3].

The use of machine learning (ML) in complete safety measures improves overall defensive capabilities, lowering the demand for human interaction while increasing reaction speed and effectiveness. ML allows security systems to automatically detect and handle threats in a constantly shifting threat environment, adjusting to new methods of attack, and offering strong defense. Through examples and practical examples, ML's effectiveness in bolstering network security is demonstrated, highlighting areas that require further development.[4].

The rapid development of network-based innovations has resulted in a more complex and dynamic risk landscape. Cybersecurity risks and events are rising because of malicious actors using advanced techniques to take advantage of weaknesses in networks and computer systems. The growing frequency of ransomware assaults, data thefts, and high-profile incursions has highlighted the fragility of digital ecosystems. This part provides a thorough analysis of the evolving threat environment in network safety, emphasizing the need for proactive and flexible security solutions.[5].

Strong security procedures are now essential due to the profound consequences of security breaches, which include monetary losses, harm to one's image, fines from the government, and endangered user privacy. As businesses depend increasingly on online resources and computer networks, the likelihood of cyberattacks is rising, making an initiative-taking cybersecurity strategy necessary. The main obstacles include the changing threat landscape, advanced attack methods, data breaches, resource limitations, adherence to regulations, and the need for flexible and scalable safety measures.[6].

Conventional security methods, like rule-based systems and signature-based detection, are becoming less and less successful in addressing the ever-changing strategies employed by malicious actors. The need for advanced and intelligent security solutions stems from the growing complexity of cyberthreats, such as social engineering and polymorphic malware. Because of its ability to recognize patterns and abnormalities, machine learning is a vital tool for enhancing security defenses. Through real-time analysis of massive datasets and the identification of

behavioral abnormalities that point to dangers, this study highlights the importance of machine learning in bolstering defenses.

1.1 Neutrosophic Set

Using a collection of criteria to evaluate options is made easier with multicriteria decision making (MCDM). This method has been used to deal with several issues in a variety of disciplines thus far. Following Bellman and Zadeh's introduction of fuzzy MCDM [7], which is based on fuzzy set theory, significant progress has been achieved in resolving complicated decision-making issues.

In fuzzy set theory, the membership function $\mu(x) \in [0,1]$ is used to demonstrate belonging to a set[8]. However, there are situations in which figuring out a set's membership with a single, clear number is difficult, especially when dealing with intricate decision-making issues. Therefore, by adding nonmembership to a set $\nu(x) \in [0,1]$, Atanassov [9] Expanded fuzzy set theory. According to Atanassov's theory, the indeterminacy of intuitionistic sets is by default. $1 - \mu(x) - \nu(x)$.

By suggesting a neutrosophic set, Smarandache [10] Expanded fuzzy sets even further. The truth-membership $T_K(x_i)$, falsity-membership $F_K(x_i)$, and indeterminacy-membership $I_K(x_i)$ Functions are the three independent membership functions that make up the neutrosophic set. By changing the constraints $T_K(x_i), I_K(x_i), F_K(x_i) \in [0, 1]$ and $0 \leq -0 \leq T_K(x_i) + I_K(x_i) + F_k(x_i)) \leq 3$, Smarandache and Wang et al. [11] Further presented a single-valued neutrosophic set that is more suited for resolving scientific and engineering issues.

It can be challenging to represent alternative evaluations using precise values when tackling some types of decision-making issues, such as those involving estimations and projections, particularly when ratings are gathered through surveys. These kinds of difficult decision-making situations may be simplified by using fuzzy sets, intuitionistic fuzzy sets, and neutrosophic fuzzy sets. However, there are certain restrictions associated with the neutrosophic set theory when it comes to the usage of fuzzy sets and intuitionistic fuzzy sets. Respondents in surveys may readily express their opinions and preferences by employing three mutually independent membership functions that are employed in neutrosophic set theory.[12], [13].

2. Neutrosophic Model

This section combines the machine learning models with the Neutrosophic numbers to select the best ML model based on a set of criteria. We apply a set of ML models, then we select the best by using the proposed approach. First, we use the single-valued Neutrosophic numbers (SVNNs) to deal with uncertainty and vague information. We show some definitions of SVNNs, then we obtain the criteria weights and rank the alternatives by using the EDAS method.

The definitions of the SVNNs are organized as follows.[14], [15]s:

Definition 1.

Neutrosophic Set has three membership functions such as truth, indeterminacy, and falsity, and can be defined as:

$$K = \{(T_K(x_i), I_K(x_i), F_K(x_i))|x_i \in X\} \quad (1)$$

Then we can meet the following conditions such as:

$$-0 \leq T_K(x_i) + I_K(x_i) + F_k(x_i) \leq 3 + \quad (2)$$

Definition 2.

We show some operations of two SVNNs, such as:

$y_1 = t_{y_1}(x), i_{y_1}(x), f_{y_1}(x)$ and $y_2 = t_{y_2}(x), i_{y_2}(x), f_{y_2}(x)$

$$y_1^c = \left(f_{y_1}(x), 1 - i_{y_1}(x), t_{y_1}(x)\right) \quad (3)$$

$$y_1 \cup y_2 = \begin{pmatrix} \max\{t_{y_1}(x), t_{y_2}(x)\}, \\ \min\{i_{y_1}(x), i_{y_2}(x)\}, \\ \min\{f_{y_1}(x), f_{y_2}(x)\} \end{pmatrix} \quad (4)$$

$$y_1 \cap y_2 = \begin{pmatrix} \min\{t_{y_1}(x), t_{y_2}(x)\}, \\ \max\{i_{y_1}(x), i_{y_2}(x)\}, \\ \max\{f_{y_1}(x), f_{y_2}(x)\} \end{pmatrix} \quad (5)$$

$$y_1 + y_2 = \begin{pmatrix} t_{y_1}(x) + t_{y_2}(x) - t_{y_1}(x)t_{y_2}(x), \\ i_{y_1}(x)i_{y_2}(x), \\ f_{y_1}(x)f_{y_2}(x) \end{pmatrix} \quad (6)$$

$$y_1 y_2 = \begin{pmatrix} t_{y_1}(x)t_{y_2}(x), \\ i_{y_1}(x) + i_{y_2}(x) - i_{y_1}(x)i_{y_2}(x), \\ f_{y_1}(x) + f_{y_2}(x) - f_{y_1}(x)f_{y_2}(x) \end{pmatrix} \quad (7)$$

$$\aleph y_1 = \left(1 - \left(1 - t_{y_1}(x)\right)^{\aleph}, \left(i_{y_1}(x)\right)^{\aleph}, \left(f_{y_1}(x)\right)^{\aleph}\right) \quad (8)$$

$$y_1^{\aleph} = \begin{pmatrix} \left(t_{y_1}(x)\right)^{\aleph}, \\ 1 - \left(1 - i_{y_1}(x)\right)^{\aleph}, \\ 1 - \left(1 - f_{y_1}(x)\right)^{\aleph} \end{pmatrix} \quad (9)$$

Then we show the steps of the MCDM approach.

First, we build the decision matrix between the criteria and alternatives. We use SVNNs to evaluate the criteria and alternatives. Then we obtain crisp values. Then we combine the decision matrix into a single matrix.

We compute the criteria weights by the average method. Then we apply the steps of the EDAS method to rank the ML models.[16], [17].

The average solution is obtained as:

$$A_j = \frac{\sum_{i=1}^{m} y_{ij}}{m} \tag{10}$$

Obtained positive and negative distances.

$$Q_{ij} = \frac{\max\left(0, \left(y_{ij} - A_j\right)\right)}{A_j} \tag{11}$$

$$U_{ij} = \frac{\max\left(0, \left(A_j - y_{ij}\right)\right)}{A_j} \tag{12}$$

$$Q_{ij} = \frac{\max\left(0, \left(A_j - y_{ij}\right)\right)}{A_j} \tag{13}$$

$$U_{ij} = \frac{\max\left(0, \left(y_{ij} - A_j\right)\right)}{A_j} \tag{14}$$

The weighted $Q_{ij}\ and\ U_{ij}$ Values are obtained, such as:

$$H_i = \sum_{j=1}^{n} Q_{ij} w_j \tag{15}$$

$$G_i = \sum_{j=1}^{n} U_{ij} w_j \tag{16}$$

The weighted normalized $H_i\ and\ G_i$ Values are obtained, such as:

$$F_i = \frac{H_i}{\max(H_i)} \tag{17}$$

$$D_i = \frac{G_i}{\max(G_i)} \tag{18}$$

The appraisal value is computed as:

$$B_i = 0.5 * (F_i + D_i) \tag{19}$$

3. Results of ML models and Neutrosophic Model

The results of the ML models are discussed in this section. This study works on the NSL-KDD dataset, which is downloaded from the Kaggle website to be analyzed.

An essential resource for data collecting is the NSL-KDD dataset, which comprises 100,000 records with details such as IP addresses, port numbers, protocol types, and packet sizes. Because it includes both legitimate and risky network activity, this dataset is essential for anomaly detection. The preprocessing stages, which include feature normalization, categorical variable encoding, and missing value management, ensure that ML models get high-quality data. Table 1 shows the details of the database. Table 2 shows some descriptions of the dataset.

Table 1. The first five rows of the dataset.

	0	**1**	**2**	**3**	**4**
DURATION	0	0	0	0	0
PROTOCOL_TYPE	UDP	TCP	TCP	TCP	TCP
SERVICE	OTHER	PRIVATE	HTTP	HTTP	PRIVATE
FLAG	SF	S0	SF	SF	REJ
SRC_BYTES	146	0	232	199	0
DST_BYTES	0	0	8153	420	0
LAND	0	0	0	0	0
WRONG_FRAGMENT	0	0	0	0	0
URGENT	0	0	0	0	0
HOT	0	0	0	0	0
NUM_FAILED_LOGINS	0	0	0	0	0
LOGGED_IN	0	0	1	1	0
NUM_COMPROMISED	0	0	0	0	0
ROOT_SHELL	0	0	0	0	0
SU_ATTEMPTED	0	0	0	0	0
NUM_ROOT	0	0	0	0	0
NUM_FILE_CREATIONS	0	0	0	0	0
NUM_SHELLS	0	0	0	0	0
NUM_ACCESS_FILES	0	0	0	0	0
NUM_OUTBOUND_CMDS	0	0	0	0	0
IS_HOST_LOGIN	0	0	0	0	0
IS_GUEST_LOGIN	0	0	0	0	0
COUNT	13	123	5	30	121
SRV_COUNT	1	6	5	32	19
SERROR_RATE	0	1	0.2	0	0
SRV_SERROR_RATE	0	1	0.2	0	0
RERROR_RATE	0	0	0	0	1
SRV_RERROR_RATE	0	0	0	0	1
SAME_SRV_RATE	0.08	0.05	1	1	0.16
DIFF_SRV_RATE	0.15	0.07	0	0	0.06
SRV_DIFF_HOST_RATE	0	0	0	0.09	0
DST_HOST_COUNT	255	255	30	255	255
DST_HOST_SRV_COUNT	1	26	255	255	19
DST_HOST_SAME_SRV_RATE	0	0.1	1	1	0.07
DST_HOST_DIFF_SRV_RATE	0.6	0.05	0	0	0.07
DST_HOST_SAME_SRC_PORT_RATE	0.88	0	0.03	0	0
DST_HOST_SRV_DIFF_HOST_RATE	0	0	0.04	0	0
DST_HOST_SERROR_RATE	0	1	0.03	0	0
DST_HOST_SRV_SERROR_RATE	0	1	0.01	0	0
DST_HOST_RERROR_RATE	0	0	0	0	1
DST_HOST_SRV_RERROR_RATE	0	0	0.01	0	1
OUTCOME	NORMAL	NEPTUNE	NORMAL	NORMAL	NEPTUNE
LEVEL	15	19	21	21	21

Table 2. Description of the dataset.

	COUNT	MEAN	STD	MIN	25%	50%	75%	MAX
DURATION	125972	287.1469	2604.526	0	0	0	0	42908
SRC_BYTES	1.26E+05	4.56E+04	5.87E+06	0.00E+00	0.00E+00	4.40E+01	2.76E+02	1.38E+09
DST_BYTES	1.26E+05	1.98E+04	4.02E+06	0.00E+00	0.00E+00	0.00E+00	5.16E+02	1.31E+09
LAND	125972	0.000198	0.014086	0	0	0	0	1
WRONG_FRAGMENT	125972	0.022688	0.253531	0	0	0	0	3
URGENT	125972	0.000111	0.014366	0	0	0	0	3
HOT	125972	0.204411	2.149977	0	0	0	0	77
NUM_FAILED_LOGINS	125972	0.001222	0.045239	0	0	0	0	5
LOGGED_IN	125972	0.395739	0.489011	0	0	0	1	1
NUM_COMPROMISED	125972	0.279253	23.94214	0	0	0	0	7479
ROOT_SHELL	125972	0.001342	0.036603	0	0	0	0	1
SU_ATTEMPTED	125972	0.001103	0.045155	0	0	0	0	2
NUM_ROOT	125972	0.302194	24.39972	0	0	0	0	7468
NUM_FILE_CREATIONS	125972	0.012669	0.483937	0	0	0	0	43
NUM_SHELLS	125972	0.000413	0.022181	0	0	0	0	2
NUM_ACCESS_FILES	125972	0.004096	0.09937	0	0	0	0	9
NUM_OUTBOUND_CMDS	125972	0	0	0	0	0	0	0
IS_HOST_LOGIN	125972	0.000008	0.002817	0	0	0	0	1
IS_GUEST_LOGIN	125972	0.009423	0.096613	0	0	0	0	1
COUNT	125972	84.10821	114.5088	0	2	14	143	511
SRV_COUNT	125972	27.73809	72.63609	0	2	8	18	511
SERROR_RATE	125972	0.284487	0.446457	0	0	0	1	1
SRV_SERROR_RATE	125972	0.282488	0.447024	0	0	0	1	1
RERROR_RATE	125972	0.119959	0.320437	0	0	0	0	1
SRV_RERROR_RATE	125972	0.121184	0.323648	0	0	0	0	1
SAME_SRV_RATE	125972	0.660925	0.439624	0	0.09	1	1	1
DIFF_SRV_RATE	125972	0.063053	0.180315	0	0	0	0.06	1
SRV_DIFF_HOST_RATE	125972	0.097322	0.259831	0	0	0	0	1
DST_HOST_COUNT	125972	182.1492	99.20657	0	82	255	255	255
DST_HOST_SRV_COUNT	125972	115.6537	110.7029	0	10	63	255	255
DST_HOST_SAME_SRV_RATE	125972	0.521244	0.44895	0	0.05	0.51	1	1
DST_HOST_DIFF_SRV_RATE	125972	0.082952	0.188922	0	0	0.02	0.07	1
DST_HOST_SAME_SRC_PORT_RATE	125972	0.148379	0.308998	0	0	0	0.06	1
DST_HOST_SRV_DIFF_HOST_RATE	125972	0.032543	0.112564	0	0	0	0.02	1
DST_HOST_SERROR_RATE	125972	0.284455	0.444785	0	0	0	1	1
DST_HOST_SRV_SERROR_RATE	125972	0.278487	0.44567	0	0	0	1	1
DST_HOST_RERROR_RATE	125972	0.118832	0.306559	0	0	0	0	1
DST_HOST_SRV_RERROR_RATE	125972	0.120241	0.31946	0	0	0	0	1
LEVEL	125972	19.50406	2.291512	0	18	20	21	21

We show the correlation between the features of the dataset by showing the heatmap as shown in Fig. 1.

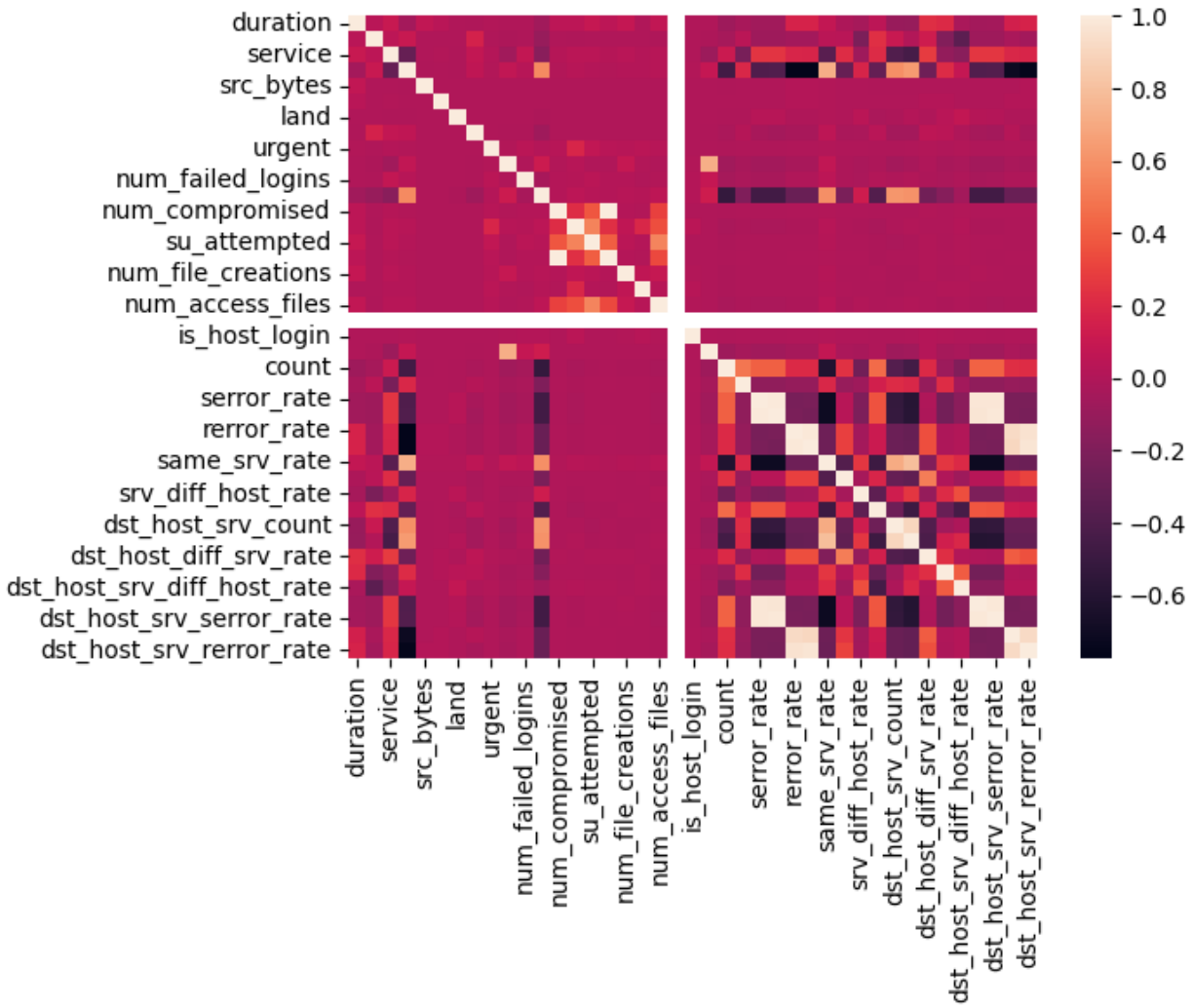

Fig 1. The heatmap of the dataset.

We use six ML models to train the dataset and obtain the best results. The machine learning models are[18], [19]:

- ✓ Random Forest Classifier (RFC)
- ✓ Logistic Regression (LR)
- ✓ Support Vector Machine (SVM)
- ✓ ExtraTrees Classifier (ETC)
- ✓ AdaBoost Classifier (ABC)
- ✓ Bagging Classifier (BC)

Then we use different evaluation metrics to evaluate these ML models, such as[20], [21]:

- ✓ Accuracy (ACC)

- ✓ Precision score (PS)
- ✓ Recall score (RS)
- ✓ F1_score (FS)
- ✓ Cohen kappa score (CKS)
- ✓ Fbeta score (FBS)
- ✓ Matthews corrcoef (MC)

We trained these ML models on the used dataset. Then we show the evaluation matrices of each ML model as shown in Table 3.

Table 3. The results of ML models.

	ACC	PS	RS	FS	CKS	FBS	MC
LR	0.970879	0.970879	0.970879	0.970879	0.953772	0.970879	0.953801
SVM	0.977107	0.977107	0.977107	0.977107	0.963786	0.977107	0.963802
RFC	0.993671	0.993671	0.993671	0.993671	0.989964	0.993671	0.989971
ABC	0.812786	0.812786	0.812786	0.812786	0.663977	0.812786	0.989549
BC	0.993402	0.993402	0.993402	0.993402	0.989547	0.993402	0.989549
ETC	0.992998	0.992998	0.992998	0.992998	0.9889	0.992998	0.988905

Then we apply the Neutrosophic methodology to show the best ML model. Table 4 shows the criteria and alternatives of this study. The alternatives are ML models, and the criteria are the evaluation matrices. We have four experts to evaluate the ML models based on their results to select the best one. We use SVNNs to evaluate the criteria and alternatives as shown in Table 5. Then we obtain crisp values. Then we combine the decision matrix. Then we obtain the criteria weights as shown in Fig. 2.

Table 4. The evaluation matrices and alternatives.

Criteria	Alternatives.
(ACC): $NADC_1$	(RFC): $NADA_1$
(PS): $NADC_2$	(LR): $NADA_2$
(RS): $NADC_3$	(SVM): $NADA_3$
(FS): $NADC_4$	(ETC): $NADA_4$
(CKS): $NADC_5$	(ABC): $NADA_5$
(FBS): $NADC_6$	(BC): $NADA_6$
(MC): $NADC_7$	

Table 5. The SVNNs.

	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
NADA 1	(0.9,0.1,0.2)	(0.8,0.2,0.3)	(0.7,0.3,0.4)	(0.6,0.4,0.5)	(0.5,0.5,0.5)	(0.4,0.5,0.6)	(0.3,0.6,0.7)

$NADA_2$	(0.9,0.1,0.2)	(0.3,0.6,0.7)	(0.4,0.5,0.6)	(0.5,0.5,0.5)	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.9,0.1,0.2)
$NADA_3$	(0.8,0.2,0.3)	(0.7,0.3,0.4)	(0.6,0.4,0.5)	(0.5,0.5,0.5)	(0.4,0.5,0.6)	(0.8,0.2,0.3)	(0.8,0.2,0.3)
$NADA_4$	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.8,0.2,0.3)	(0.9,0.1,0.2)	(0.3,0.6,0.7)	(0.9,0.1,0.2)	(0.7,0.3,0.4)
$NADA_5$	(0.5,0.5,0.5)	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.8,0.2,0.3)	(0.9,0.1,0.2)	(0.3,0.6,0.7)	(0.6,0.4,0.5)
$NADA_6$	(0.5,0.5,0.5)	(0.5,0.5,0.5)	(0.6,0.4,0.5)	(0.5,0.5,0.5)	(0.3,0.6,0.7)	(0.4,0.5,0.6)	(0.5,0.5,0.5)
	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
$NADA_1$	(0.6,0.4,0.5)	(0.8,0.2,0.3)	(0.7,0.3,0.4)	(0.6,0.4,0.5)	(0.5,0.5,0.5)	(0.4,0.5,0.6)	(0.3,0.6,0.7)
$NADA_2$	(0.7,0.3,0.4)	(0.3,0.6,0.7)	(0.4,0.5,0.6)	(0.6,0.4,0.5)	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.6,0.4,0.5)
$NADA_3$	(0.8,0.2,0.3)	(0.7,0.3,0.4)	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.6,0.4,0.5)	(0.8,0.2,0.3)	(0.7,0.3,0.4)
$NADA_4$	(0.9,0.1,0.2)	(0.7,0.3,0.4)	(0.8,0.2,0.3)	(0.8,0.2,0.3)	(0.7,0.3,0.4)	(0.9,0.1,0.2)	(0.8,0.2,0.3)
$NADA_5$	(0.3,0.6,0.7)	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.9,0.1,0.2)	(0.8,0.2,0.3)	(0.3,0.6,0.7)	(0.9,0.1,0.2)
$NADA_6$	(0.6,0.4,0.5)	(0.6,0.4,0.5)	(0.6,0.4,0.5)	(0.3,0.6,0.7)	(0.9,0.1,0.2)	(0.6,0.4,0.5)	(0.3,0.6,0.7)
	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
$NADA_1$	(0.9,0.1,0.2)	(0.8,0.2,0.3)	(0.7,0.3,0.4)	(0.6,0.4,0.5)	(0.5,0.5,0.5)	(0.4,0.5,0.6)	(0.3,0.6,0.7)
$NADA_2$	(0.3,0.6,0.7)	(0.3,0.6,0.7)	(0.4,0.5,0.6)	(0.5,0.5,0.5)	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.9,0.1,0.2)
$NADA_3$	(0.4,0.5,0.6)	(0.9,0.1,0.2)	(0.6,0.4,0.5)	(0.5,0.5,0.5)	(0.4,0.5,0.6)	(0.8,0.2,0.3)	(0.3,0.6,0.7)
$NADA_4$	(0.5,0.5,0.5)	(0.3,0.6,0.7)	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.4,0.5,0.6)
$NADA_5$	(0.6,0.4,0.5)	(0.4,0.5,0.6)	(0.3,0.6,0.7)	(0.9,0.1,0.2)	(0.3,0.6,0.7)	(0.9,0.1,0.2)	(0.5,0.5,0.5)
$NADA_6$	(0.7,0.3,0.4)	(0.5,0.5,0.5)	(0.4,0.5,0.6)	(0.3,0.6,0.7)	(0.4,0.5,0.6)	(0.3,0.6,0.7)	(0.6,0.4,0.5)
	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
$NADA_1$	(0.4,0.5,0.6)	(0.3,0.6,0.7)	(0.8,0.2,0.3)	(0.3,0.6,0.7)	(0.5,0.5,0.5)	(0.6,0.4,0.5)	(0.3,0.6,0.7)
$NADA_2$	(0.3,0.6,0.7)	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.6,0.4,0.5)	(0.7,0.3,0.4)	(0.9,0.1,0.2)
$NADA_3$	(0.3,0.6,0.7)	(0.8,0.2,0.3)	(0.3,0.6,0.7)	(0.8,0.2,0.3)	(0.7,0.3,0.4)	(0.8,0.2,0.3)	(0.8,0.2,0.3)
$NADA_4$	(0.8,0.2,0.3)	(0.8,0.2,0.3)	(0.8,0.2,0.3)	(0.5,0.5,0.5)	(0.7,0.3,0.4)	(0.8,0.2,0.3)	(0.5,0.5,0.5)
$NADA_5$	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.9,0.1,0.2)	(0.8,0.2,0.3)	(0.9,0.1,0.2)	(0.8,0.2,0.3)

NADA$_6$	(0.3,0.6,0.7)	(0.3,0.6,0.7)	(0.3,0.6,0.7)	(0.8,0.2,0.3)	(0.9,0.1,0.2)	(0.3,0.6,0.7)	(0.9,0.1,0.2)

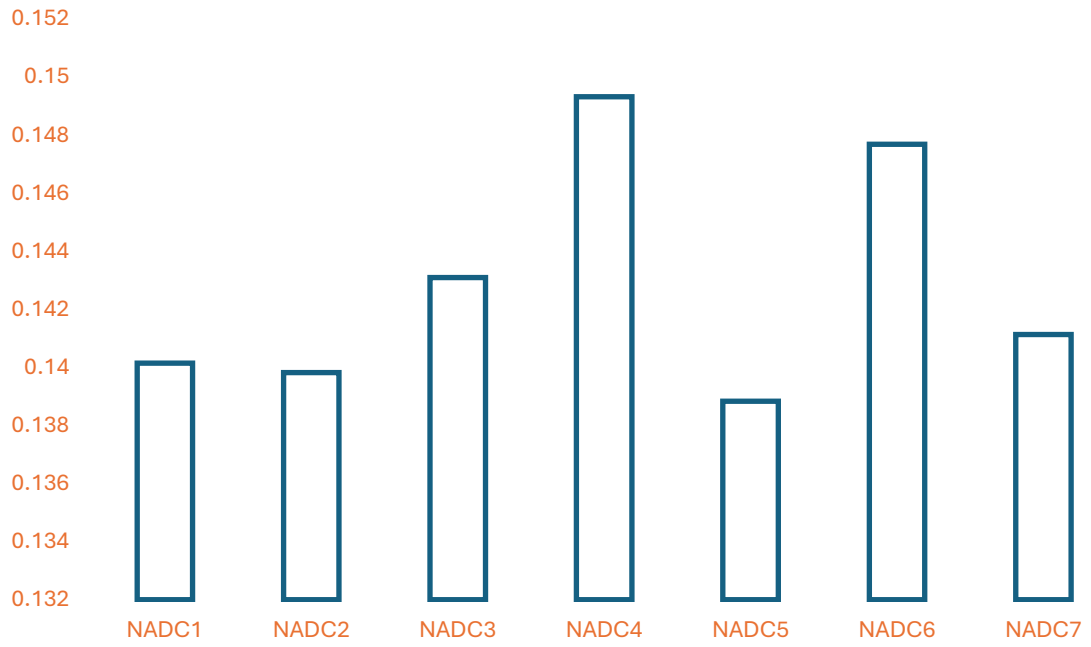

Fig 2. The weight of evaluation matrices.

Then we apply the steps of the EDAS method under the SVNNs to show the best ML model in this dataset. We obtain the average solution using Eq. (10).

Then we obtained positive and negative distances using Equations. (11-14) as shown in Tables 6-7.

Then we obtained the weighted. Q_{ij} *and* U_{ij} Values using Eq. (15 and 16) as shown in Tables 8-9.

Then we obtained the weighted normalized. H_i *and* G_i Values are obtained using equations (17 and 18).

Then we obtained the appraisal value is computed using Eq. (19). Then we rank the alternatives as shown in Fig. 3.

Table 6. The positive distance values.

	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
$NADA_1$	0.149533	0.11007	0.139588	0	0	0	0
$NADA_2$	0	0	0	0	0	0.064302	0.322506

$NADA_3$	0	0.250585	0	0	0	0.223947	0.058005
$NADA_4$	0.135514	0.025761	0.304348	0.184211	0.075472	0.343681	0
$NADA_5$	0	0.025761	0.043478	0.328947	0.160377	0	0.12761
$NADA_6$	0	0	0	0	0.061321	0	0

Table 7. The negative distance values.

	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
$NADA_1$	0	0	0	0.197368	0.150943	0.254989	0.443155
$NADA_2$	0.074766	0.213115	0.107551	0.039474	0.037736	0	0
$NADA_3$	0.03271	0	0.162471	0.039474	0.108491	0	0
$NADA_4$	0	0	0	0	0	0	0.011601
$NADA_5$	0.046729	0	0	0	0	0.042129	0
$NADA_6$	0.130841	0.199063	0.217391	0.236842	0	0.334812	0.053364

Table 8. The weighted Q_{ij} values.

	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
$NADA_1$	0.020956	0.01539	0.019974	0	0	0	0
$NADA_2$	0	0	0	0	0	0.009496	0.045514
$NADA_3$	0	0.035036	0	0	0	0.033071	0.008186
$NADA_4$	0.018991	0.003602	0.043549	0.027505	0.010478	0.050753	0
$NADA_5$	0	0.003602	0.006221	0.049116	0.022266	0	0.018009
$NADA_6$	0	0	0	0	0.008513	0	0

Table 9. The weighted U_{ij} Values.

	$NADC_1$	$NADC_2$	$NADC_3$	$NADC_4$	$NADC_5$	$NADC_6$	$NADC_7$
$NADA_1$	0	0	0	0.02947	0.020956	0.037656	0.062541
$NADA_2$	0.010478	0.029797	0.01539	0.005894	0.005239	0	0
$NADA_3$	0.004584	0	0.023248	0.005894	0.015062	0	0
$NADA_4$	0	0	0	0	0	0	0.001637
$NADA_5$	0.006549	0	0	0	0	0.006221	0
$NADA_6$	0.018337	0.027832	0.031107	0.035363	0	0.049443	0.007531

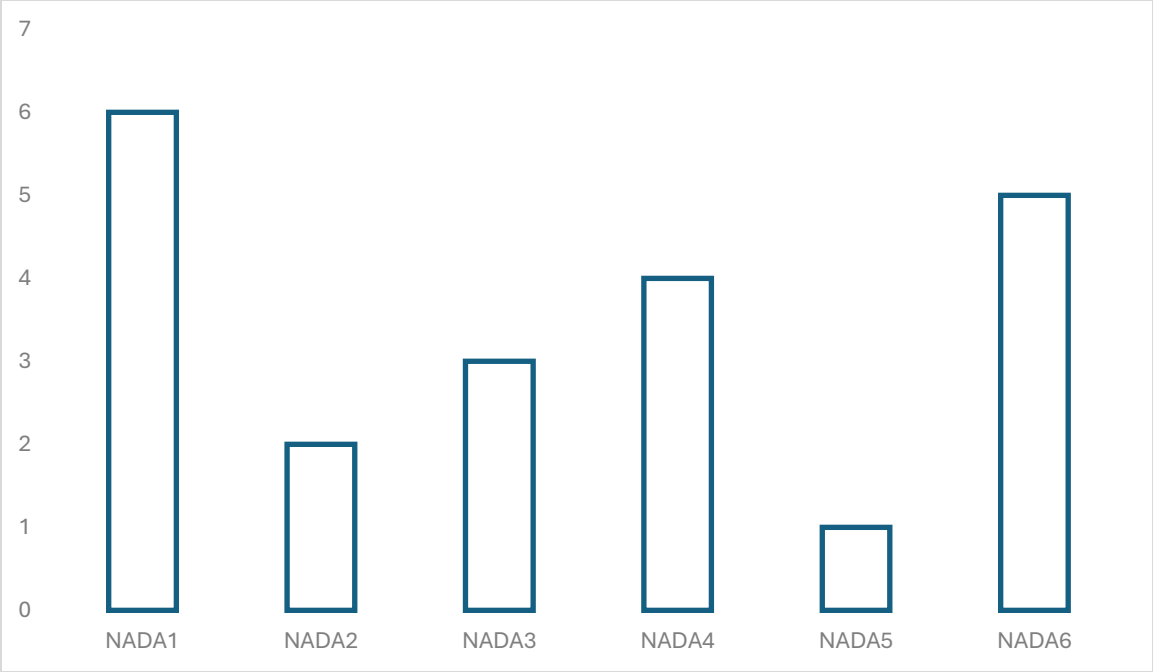

Fig 3. Ranks of the ML models.

From the results of the proposed Neutrosophic Framework, we show that the RFC is the best ML model based on different evaluation methods.

4. Conclusions

ML-driven techniques for identifying network abnormalities have been thoroughly examined in this study. The study acknowledged and resolved the drawbacks of traditional security measures, emphasizing the calculated use of ML techniques such as SVM, LR, RFC, and ensemble models. Evaluation matrices such as ACC, PS, FS, and others show that the ML model performed well. The plan emphasized how network security risks are always changing and how machine learning can be used to address them. Then we used the Single-valued Neutrosophic Numbers (SVNNs) framework to select the best ML model based on the different evaluation matrices. We used the MCDM approach, such as the EDAS method, to compute the criteria weights and rank the ML models. The SVNNs are used to deal with uncertainty and vague information. The results show the RFC is the best ML model under different evaluation methods.

References

[1] G. Sun, Z. Xu, H. Yu, X. Chen, V. Chang, and A. V. Vasilakos, "Low-latency and resource-efficient service function chaining orchestration in network function virtualization," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5760–5772, 2019.

[2] M. Dai, G. Sun, H. Yu, and D. Niyato, "Maximize the long-term average revenue of network slice provider via admission control among heterogeneous slices," *IEEE/ACM*

Trans. Netw., vol. 32, no. 1, pp. 745–760, 2023.

[3] R. Liu, J. Shi, X. Chen, and C. Lu, "Network anomaly detection and security defense technology based on machine learning: A review," *Comput. Electr. Eng.*, vol. 119, p. 109581, 2024.

[4] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Commun. Surv. tutorials*, vol. 16, no. 1, pp. 303–336, 2013.

[5] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, 2016.

[6] G. Fernandes, J. J. P. C. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, "A comprehensive survey on network anomaly detection," *Telecommun. Syst.*, vol. 70, pp. 447–489, 2019.

[7] R. E. Bellman and L. A. Zadeh, "Decision-making in a fuzzy environment," *Manage. Sci.*, vol. 17, no. 4, p. B-141, 1970.

[8] L. A. Zadeh, "Fuzzy sets," *Inf. Control*, vol. 8, no. 3, pp. 338–353, 1965.

[9] K. T. Atanassov and K. T. Atanassov, *Intuitionistic fuzzy sets*. Springer, 1999.

[10] F. Smarandache, "Neutrosophy: neutrosophic probability, set, and logic: analytic synthesis & synthetic analysis," 1998.

[11] H. Wang, F. Smarandache, Y. Zhang, and R. Sunderraman, "Single valued neutrosophic sets," *Infin. Study*, vol. 12, 2010.

[12] H. Huang, "New distance measure of single-valued neutrosophic sets and its application," *Int. J. Intell. Syst.*, vol. 31, no. 10, pp. 1021–1032, 2016.

[13] R. Şahin and A. Küçük, "Subsethood measure for single-valued neutrosophic sets," *J. Intell. Fuzzy Syst.*, vol. 29, no. 2, pp. 525–530, 2015.

[14] H.-L. Yang, C.-L. Zhang, Z.-L. Guo, Y.-L. Liu, and X. Liao, "A hybrid model of single valued neutrosophic sets and rough sets: single valued neutrosophic rough set model," *Soft Comput.*, vol. 21, pp. 6253–6267, 2017.

[15] S. Pramanik, "Single-Valued Neutrosophic Set: An Overview," *Transdisciplinarity*, pp. 563–608, 2022.

[16] D. Stanujkić *et al.*, "A single-valued neutrosophic extension of the EDAS method," *Axioms*, vol. 10, no. 4, p. 245, 2021.

[17] D. Xu, X. Cui, and H. Xian, "An extended EDAS method with a single-valued complex neutrosophic set and its application in green supplier selection," *Mathematics*, vol. 8, no. 2, p. 282, 2020.

[18] X.. Dong, Z. Yu, W. Cao, Y. Shi, and Q. Ma, "A survey on ensemble learning," *Front. Comput. Sci.*, vol. 14, pp. 241–258, 2020.

[19] D. A. Salazar, J. I. Vélez, and J. C. Salazar, "Comparison between SVM and logistic regression: Which one is better to discriminate?" *Rev. Colomb. Estadística*, vol. 35, no. 2, pp. 223–237, 2012.

[20] F. Pistorius, D. Grimm, F. Erdösi, and E. Sax, "Evaluation matrix for smart machine-learning algorithm choice," in *2020 1st International Conference on Big Data Analytics and Practices (IBDAP)*, IEEE, 2020, pp. 1–6.

[21] G. S. Handelman *et al.*, "Peering into the black box of artificial intelligence: evaluation metrics of machine learning methods," *Am. J. Roentgenol.*, vol. 212, no. 1, pp. 38–43, 2019.

Received: Nov. 3, 2024. Accepted: April 1, 2025