Extended Fuzzy Neutrosophic Classifier for Accurate Intrusion Detection and Classification

Mohamed Elhoseny[1,*], Mahmoud Abdel-salam[2], Ibrahim M. Elhasnony[2]

[1]University of Sharjah, Sharjah, United Arab Emirates
[2]Faculty of Computer and Information, Mansoura University, Mansoura, Egypt
Emails: melhoseny@ieee.org; mahmoud20@mans.edu.eg; ibrahimhesin2005@mans.edu.eg

Abstract

Intrusion Detection is crucial in contemporary cybersecurity landscapes to proactively thwart and identify possible threats. The risk of data breaches, malicious activities, and unauthorized access escalates as organizations increasingly rely on interconnected systems. Intrusion Detection Systems (IDS) are imperative for the continuous monitoring of system and network activities, quickly identifying patterns or anomalies indicative of cyber threats. IDS acts as a frontline defense mechanism with the ability to identify abnormal behaviors and known attack signatures. Prompt recognition allows for safeguarding sensitive data, timely response, fortifying the overall resilience of IT infrastructures, and reducing the effect of security incidents. The implementation of robust IDS is vital in an era marked by evolving cyber threats to ensure the confidentiality, availability, and integrity of digital assets. This study develops an improved Arithmetic Optimization Algorithm with an Extended Fuzzy Neutrosophic Classifier technique (AOA-EFNSC) for Accurate Intrusion Detection and Classification. The main goal of proposing this model is to recognize the presence of intrusions effectually. A min-max scalar is applied to normalize the input data before using the improved AOA as a feature selection method. For intrusion detection, the proposed model uses the FNSC technique for the recognition and classification of the intrusions. A sequence of experimentations was involved to validate the superior performance of the proposed model. The experimental value pointed out that our proposed approach outperforms the previous models and enhances the intrusion detection results.

Keywords: Intrusion Detection System; Cyberattack; Arithmetic Optimization Algorithm; Neutrosophic Classifier; Fuzzy Logic

1. Introduction

The wide-range acceptance of cutting-edge techniques like the Internet of Things (IoT), big data (BD), and the flexible computing and storage source of cloud computing (CC) has been directed to the domain perceiving data overflow, the significance of the concurrent huge data generation by IoT and humans [1]. Therefore, altering society and the domain of business in several features. According to McKinsey, the reasonable power in the inclusive market is presently focused on connecting effectual and creative BD and cutting-edge techniques [2]. So, creating these setups will not only draw consideration from the business and government industries but similarly from illegal efforts to approach these complex and valued data [3]. However, these valuable data are normally restricted in numerous BD and applications of the real world, which are classified into symmetric and asymmetric data distributions. For example, the symmetric relations between the data of social systems and the asymmetric prospect supply of regular and malicious network traffic. The lost data within these real uses are quite rich in unseen patterns and data [4]. So, creating effectual and actual measures of filtering these valued patterns is important.

Similarly, the rising reliance on the internet and its amenities has headed a determined danger against computer systems [5]. For example, numerous types of cyberattacks have been changed radically since the origin of the internet and the fast increase of innovative technologies. Regardless of the tireless struggles of safety professionals in terms of defence mechanisms, hackers have constantly originated methods to acquire away directed sources from valued and most reliable resources globally by beginning sophisticated, flexible, and automatic cyberattacks [6]. As an outcome, this creates a great disaster for businesses, governments, and for people. For example, the

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

authors have been enchantingly present a brief of numerous cyberattacks and their values. At first, the paper emphasizes the prediction of 6 trillion US dollars of cybercrimes and the numerous worldwide innovative cybercrimes that main to the damage of one billion US dollars worldwide [7]. At last, an enormous 1.5 trillion US dollars of cyberattack profits result from 2 to 5 million computers negotiated every day. Then, the past few years have seen the high reputation of Intrusion Detection Systems (IDS) as an outcome of their characteristic aptitude to perceive an intrusion. With the upsurge in the use of the Internet, a massive amount of data is swapped between dissimilar communication devices [8]. The data must be communicated firmly among the collaborating devices and so, network safety is one of the leading study fields for the present network scenario. IDS are generally utilized along with other safety devices like access control and firewalls. The leading safety challenge in CC is the recognition and frustration of network attacks [9]. Currently, network intrusions have increased owing to inadequate countermeasures, and an IDS can able to tackle these safety concerns [10]. But, before using any IDS technique in a cloud atmosphere, it is vital to certify that the projected method is well developed and implemented.

This study proposes an improved Arithmetic Optimization Algorithm with an Extended Fuzzy Neutrosophic Classifier technique for Accurate Intrusion Detection and Classification. The main goal of AOA-EFNSC method is to recognize the presence of intrusions effectually. In the AOA-EFNSC technique, a min-max scalar is applied to normalize the input data. Besides, the AOA-EFNSC technique employs AOA-based feature selection technique to select a subset of feature. For intrusion detection, the AOA-EFNSC technique uses the FNSC technique for the recognition and identification of the intrusions. The experimental values pointed out that the AOA-EFNSC technique gains enhanced detection results over other models. The contribution of this study can be summarized as follows:

- An improved binary variant of AOA algorithm is proposed to enhance the global search ability of AOA.
- The novel AOA algorithm can escape from the local optimal solutions and seek for the best set of features for the classification and detection tasks.
- The EFNSC algorithm is utilized as a classifier along with the improved AOA for the classification problem in intrusion detection system.
- A set of comprehensive experiments are conducted to validate and assess the performance of the proposed AOA-EFNSC for feature selection in intrusion detection problem.

2. Literature Review

This section presents a set of recent related works applied to the feature selection problem in intrusion detection domain to highlight the research gap of the proposed work.

Park et al. [11] presented a graph-based intrusion detection and classification system termed as G-IDCS, which derives to improve the security of in-vehicle controller area network (CAN) protocol. Presenting IDSs utilizing graph model suffer from limitations like require a huge amount of CAN messages for recognition and being ineffectual for classifying attack types despite analysing several messages. In the meantime, ML or DL-based approaches are restricted sensitivity to environmental alterations like attack type alter because of the model overfitting and are ineffective give explanations for classification decisions. Fayed et al. [12] implemented a wide-ranging occupancy recognition model that trusts on an innovative fusion method for combining heterogeneous sensor data that extremely increases occupancy recognition effectiveness. By employing Neutrosophy, the developed method controls the sensor information uncertainty. Moreover, it enhances dependability by combining various sensor data. Since, it employs a single feature produced from combining numerous sensors data, testing, and training time will be minimized. In [13], an improved technique was presented employing an extreme gradient boosting (XGB) method with correlation-based FS for precise IDSs. The XGB method was employed, and it utilizes the max-depth factor as a given standard for minimizing the trees and increasing the efficiency considerably. The developed method chooses the preeminent value of the max-depth factor by exploiting a comprehensive search optimization method.

Zainudin et al. [14] examined federated learning (FL)-based low-complexity intrusion detection and classification in SDN-enabled industrial CPS. This method employs Chi-square and Pearson correlation coefficient (PCC) FS approaches for selecting potential features that support to decrease the model's complexity and improve result. Prasad et al. [15] projected an improved IDS for the mobile ad-hoc network. This technique mostly produces 11 sub-datasets as well as assesses their quality employing a fuzzy logic (FL) model. A probabilistic method was proposed for feature ranking. The following method extracts ineffectual features in the training and testing sets. The technique implemented a Bayesian rough set method that categorizes the behavior of mobile nodes employing received packets. The Bayes algorithm was also exploited.

Mojtaba Eskandari et al. [26] developed an anomaly-based Intrusion Detection System (IDS) model for IoT edge devices called Passban. This efficient IDS is designed to connect directly to IoT devices and can be deployed on

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

inexpensive IoT gateways, which is a unique feature of the proposed system. By leveraging the full potential of the edge computing structure, Passban effectively detects cyber threats from related data sources. It is capable of accurately identifying various types of malicious traffic, including SYN flood attacks, HTTP attacks, port scanning, and SSH brute force attacks, while maintaining a low false-positive rate.

Bakro et al. [27] developed an improved cloud-based Intrusion Detection System (IDS) incorporating Synthetic Minority Over-sampling Technique (SMOTE) to tackle issues with imbalanced data. For feature selection (FS), they utilized a hybrid approach that integrates three models: Particle Swarm Optimization (PSO), Chi-Square (CS), and Information Gain (IG). Finally, they employed the Random Forest (RF) algorithm to detect and classify various types of attacks.

In [16], a method to identify animals was presented employing establishments in DL system. Utilizing this DL technology, it has the potential to detect animals and ensure adequate security measures are in place to mitigate the risk of animals gaining entry and causing harm. This work contains image pre-processing and AI for animal recognition, species classification, and automatic animal detection utilizing CNN, alarm unit, and animal repellent circuit format. Abdelhafeez et al. [17] developed a new hybrid DL-based layer-fusion and neutrosophic-set (NS) method having two phases. Primarily, improving the classification accuracy of the trained models separately. This developed feature fusion technique was employed. The error-correcting output codes (ECOC) model has been deployed for making a category of trained true and false SVM algorithms by using integrated GoogleNet and DarkNet feature maps, correspondingly. The coding matrices of ECOC have been developed for training all true classifiers and their opponent in one to another way.

In [28], Alkanhel et al. introduced a hybrid optimization method for feature selection in Intrusion Detection Systems (IDS). This approach combines dipper-throated optimization (DTO) with grey wolf (GW) techniques and is referred to as GWDTO. The proposed model achieves a better balance between the exploitation and exploration phases of the optimization process, leading to enhanced performance.

Hassan et al. [29] created an Intrusion Detection (ID) model using an enhanced Binary Manta-Ray Foraging (BMRF) Optimizer, which is based on the S-shape function and Random Forest (RF) approach. The BMRF is primarily aimed at identifying important features and eliminating irrelevant or redundant ones in ID datasets. The RF technique is then used to evaluate these features and build the ID model. In [15], an efficient wrapper feature technique was developed to improve results and reduce computation time for IDS. This method utilizes a differential evaluation technique to select effective features, followed by an Extreme Learning Machine (ELM) classification model to analyze the chosen features.

Kareem et al. [30] developed an effective feature selection (FS) method by improving the performance of the Gorilla Troops Optimizer (GTO) using the Bird Swarm Algorithm (BSA). The BSA is utilized to enhance efficiency, leveraging the GTO in the newly designed GTO-BSA, which excels at identifying optimal solutions. Zhao et al. [18] created a hybrid Intrusion Detection (ID) system based on weighted stacking classification and the CFS-DE FS method. To reduce feature dimensions, they designed the CFS-DE algorithm to find the optimal feature subset. Subsequently, the weighted stacking technique is used to enhance the weights of the best-performing base classification models and reduce the influence of underperforming ones, thus improving classification performance.

Subramani and Selvi [31] introduced a resilient Intrusion Detection System (IDS) aimed at identifying intruders within IoT-enabled wireless sensor networks to manage security breaches. Their approach involved developing an intelligent IDS using a rule-based model combined with a Multi-Objective Particle Swarm Optimization (PSO) enabled Feature Selection (FS) technique. Additionally, they proposed an enhanced multiclass Support Vector Machine (SVM) classifier, which leverages intelligent rules to accurately detect intrusions.

Kamalesh and Muthukrishnan [32] proposed a Dictionary-based Sparse Regression Learning method enhanced with Golden Jackal Optimization (DSRL-GJO) to monitor healthcare data within an IoT-based context-aware architecture. This approach, referred to as DSRL-GJO-HD-CAA-IOT, employs structural interval gradient filtering (SIGF) for processing. Features are extracted using a structured optimal graph-based sparse feature extraction technique. These extracted features are then fed into the Dictionary-based Sparse Regression Learning model, which is optimized using the GJO method.

Alshehri [18] introduces a 2-stage hybrid multi-stage decision-making model that is depends on type-2 neutrosophic numbers (T2NNs). Primarily, this method is defining the weights of condition by the AHP methodology in the T2NN environment. Secondary, the T2NN-based Multi-Attributive Border Approximation Area Comparison (MABAC) system was utilized for ranking the several fog security methods that work on IoT environments. Chinnasamy and Rajasekaran [19] manage uncertainty data by presenting a multi-valued neutrosophic ConvLSTM (MVN-ConvLSTM) that extracts distinct deep features. MVN-ConvLSTM utilizes a

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

neutrosophic set (NS) that assumed as truth (T), indeterminacy (I), and falsity (F) memberships of all the features. Mirza and Samak [20] develops a unique system to accurately classify X-ray imageries of chest in COVID19 forecast by integrating Neutrosophic FL (NFL) with Hybrid CNN and LSTM framework. Medical image analysis contains uncertainty and imprecise data that is managed using NFL. Dias et al. [21] introduces the Rule Generator (RUGE) structure that automates the rule mining and selective method utilizing a GA with single-valued neutrosophic cross-entropy fitness operator.

Based on the review, it is evident that various metaheuristic optimization and machine learning algorithms have been employed for network intrusion detection. However, these algorithms often face challenges, such as getting trapped in local optima. Additionally, according to the No Free Lunch theorem by Ebrahimpour and Eftekhari [33], no single algorithm can solve all optimization problems. Therefore, this study proposes an Improved Binary Arithmetic Optimization Algorithm (BMRF) based attribute selection method combined with a EFNSC classifier for network intrusion detection.

3. Research Background

A. Arithmetic Optimization Algorithm

Abualigah et. al. introduced a new population-based meta-heuristic algorithm called AOA that exploits four arithmetical operators such as Addition ($A\varepsilon + \varepsilon$), Multiplication ($M\varepsilon \times \varepsilon$), Division ($D\varepsilon \div \varepsilon$), and Subtraction ($S\varepsilon - \varepsilon$) [23]. Using the following expression, the initial population is randomly generated in AOA:

$$x = LB + (U - L) \times \partial \tag{1}$$

In Eq. (1), x denotes the solution of population. The upper and lower boundaries of the search range are represented as U and L, correspondingly. ∂ denotes the randomly generated parameter lies within $[0,1]$.

The selection of exploitation and exploration is performed based on the result of MOA (Math Optimizer Accelerated) function before the commencement of AOA that can be evaluated as follows:

$$MOA(C\_Iter) = \text{Min} + C\_Iter \times \left(\frac{\text{Max} - \text{Min}}{M\_Iter}\right) \tag{2}$$

In Eq. (2), $MOA(C\_Iter)$ denotes the functional outcome at t^{th}iteration. C_Iter shows the existing iteration that lies within 1 and the maximal iteration count (M_Iter). The minimum and maximum values of MOA are represented by Min and Max. The global search or exploration in AOA is implemented by applying Multiplication (M) and Division (D) operators-based search approaches as follows:

$$x_{i,j}(t+1) = \begin{cases} best(x_j) \div (MoPr + \epsilon) \times \left(\left(U_j - L_j\right) \times \mu + L_j\right), & rand2 < 0.5 \\ best(x_j) \times (MoPr) \times \left(\left(U_j - L_j\right) \times \mu + L_j\right), & Otherwise \end{cases} \tag{3}$$

In Eq. (3), $x_i(t+1)$ characterizes the i^{th} solution of $(t+1)th$ iteration, $x_{i,j}(t)$ signifies the j^{th} location of the i^{th} individuals at the existing generation. $best(x_j)$ denotes the j^{th} position of the best solution obtained. ϵ indicates the small positive integer, the lower and upper bounds of j^{th} location is signified as L_j and U_j, correspondingly. A control parameter μ is fixed as 0.5. The Math Optimizer Probability ($MoPr$) is a coefficient that evaluated by Eq. (4):

$$MoPr(t) = 1 - \frac{t^{\frac{1}{\theta}}}{M\_Iter^{\frac{1}{\theta}}} \tag{4}$$

Where $MoPr(t)$ shows the value of $MoPr$ at t^{th} iteration. M_1ter represents the maximal iteration count. θ is a crucial variable that control the exploitation efficacy over the iteration.

Algorithm 1. Procedure of AOA
Initialize variables μ and θ. Take $\tau = 0$.
Initialize the n number of solutions position at random according to Eq. (1)
While (ending criteria is not met) do

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

Evaluate the fitness value of the generated solution.

Save the optimum solution obtained.

Eq. (2) modifies the $MoAc$ value.

Eq. (4) modifies the $MoPr$ value.

for ($i = l$ to Solutions) do

for ($J = 1$ to Positions) do

Produce a random values ($randl, rand2, and\ rand3$) within [0,1].

If ($randl > MoAc$)

If(rand2 > 0.5)

(1) Apply the Division operator (D^t" ÷ ").

Using the first rule of Eq. (3), update i^{th} solutions' position.

Else

(2) Apply the Multiplication operator (M" × ")

Using the second rule of Eq. (3) update the i^{th} solutions' position.

End if

Else

if ($r3 > 0.5$)

(1) Apply the Subtraction operator (S " − ").

Using the first rule of Eq. (5), update the i^{th} solutions' position.

else

(2) Apply the Addition operator (A " + ").

Using the second rule of Eq. (5), update the i^{th} solutions' position.

End if

End if

End for

End for

$r = r + 1$

End While

Return the global optimum solution.

In AOA, the exploitation approach is performed by using Addition (A) or Subtraction (S) operators.

$$x_{i,j}(t+1) = \begin{cases} best(x_j) - (MoPr) \times \left((U_j - L_j) \times \mu + L_j \right), rand3 < 0.5 \\ best(x_j) + (MoPr) \times \left((U_j - L_j) \times \mu + L_j \right), Otherwise \end{cases} \quad (5)$$

Where a constant μ is set as 0.5. Fig. 2 demonstrates the steps involved in AOA and presented in Algorithm 1.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

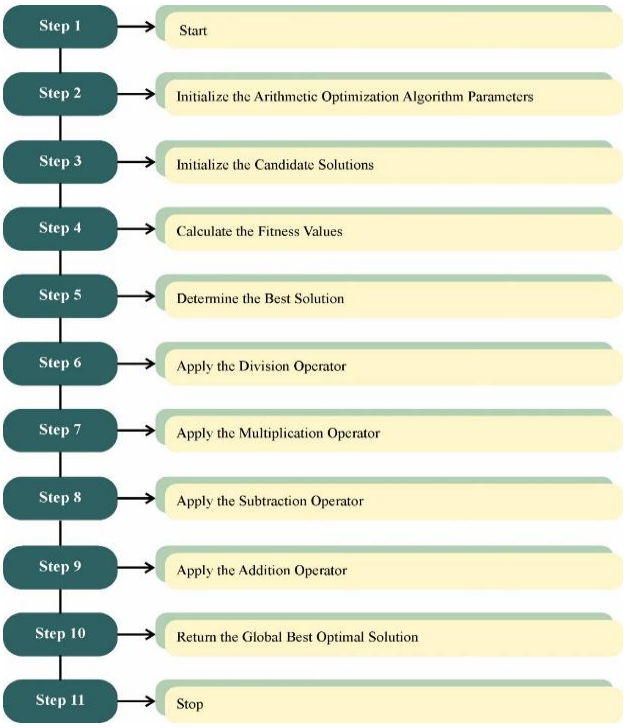

Figure 2: Steps involved in AOA.

B. Proposed binary Arithmetic Optimization Algorithm (BAOA)

The proposed binary Arithmetic Optimization Algorithm optimization algorithm utilizes an adaptive S-shaped transfer function. Below is a detailed description of the proposed algorithm.

The original Arithmetic Optimization Algorithm (AOA), introduced by [23], addresses continuous optimization problems. However, in attribute selection, attributes are binary (selected or not selected), necessitating a binary representation for the attribute space [34]. Therefore, we propose the binary Arithmetic Optimization Algorithm (AOA) algorithm, which is more suitable for binary attribute spaces. This transformation is achieved by using an adaptive S-shaped transfer function (ASSTF), making the BAOA appropriate for feature selection tasks [35]-[37].

In the BAOA algorithm, each agent (M) is represented by a sequence of binary values, forming a candidate solution. Here, n is the dimension, and each element is either 1 (attribute selected) or 0 (attribute not selected). Unlike the AOA, which updates positions through continuous stages, the BAOA algorithm updates positions by adjusting probabilities. The S-shaped transfer function is a fundamental and effective method for converting continuous values to binary states [38]. Example, take the first function, the common conversion method is as in Eq. (6) and Eq. (7)

$$\text{SSTF}\left(q_n^{iter}\right) = \frac{1}{1+e^{-\left(q_n^{iter}\right)}} \tag{6}$$

$$q_n^{\text{iter}+1} = \begin{cases} 0 \text{ if rand } < \text{SSTF}\left(q_n^{\text{iter}}\right) \\ 1 \text{ if rand } \geq \text{SSTF}\left(q_n^{iter}\right) \end{cases} \tag{7}$$

This paper introduces the proposed Binary Arithmetic Optimization Algorithm (BAOA) algorithm, enhanced with an adaptive S-shaped transfer function (ASSTF). The ASSTF adjusts based on the iterations of the BAOA algorithm, dynamically modifying the gradient to achieve a refined turnover probability. The ASSTF at the current position (x) can be represented by Eqs. (8) and (9), with the new position being computed using Eq. (9).

$$\text{ASSTF}\left(q_n^{\text{iter}}\right) = \frac{1}{1+e^{\frac{-\left(q_n^{iter}\right)}{k}}} \tag{8}$$

$$k = \left(1 - \frac{\text{iter}}{\text{MaxIter}}\right) * \text{MaxIter}_{\max} + \frac{\text{iter}}{\text{MaxIter}} * \text{MaxIter}$$

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

$$q_n^{\text{iter}+1} = \begin{cases} 0 \text{ if rand } < ASSTF(q_n^{\text{iter}}) \\ 1 \text{ if rand } \geq \text{ASSTF } (q_n^{\text{iter}}) \end{cases} \quad (9)$$

In this context, $iter$ represents the current iteration of the algorithm, while $MaxIter$ denotes the maximum number of iterations allowed. During the initial iterations, a larger value of k leads to a smaller gradient in the curve, resulting in a lower probability of change. This behavior enhances the algorithm's focus on exploitation, aiming to exploit the current solutions effectively. As the algorithm progresses to later iterations and k decreases, the gradient of the curve steepens. This causes the change probability to increase, shifting the algorithm's focus towards exploration, enabling it to escape from suboptimal local solutions and potentially find better global solutions.

C. Fundamentals of Neutrosophic Logic

A fuzzy set (FS) differs from a traditional set in that it assigns a membership level to each of its components. Based on traditional set, the logic depends on the real values such as "true" and "false" are sometimes not enough for determining the human choices. On the other hand, assumed only 2 real values, FL takes the total range from 1 ('true') and 0 ('false') for higher outcome. A FS allows its members or elements to take several levels of membership from the range of zero and one. But FS model, it needs that detected that the clarification of sets varies depends on context. Then the fuzzy morphological word 'tall' takes one classify of FS but determining the height of construction and second classify of FS once determining the human height.

Definition1. Let X refers the group of universal and $x \in X$, then FS $\hat{A}$ in X is defined as $\hat{A} = \{(x, \mu_{\hat{A}}(x)) : \mu_{\hat{A}}(x) \in [0,1], x \in X\}$, the $\mu_{\hat{A}}(x)$ is named as level of membership of x in $\hat{A}$. Then, $\mu_{\hat{A}}(x)$ represents the membership level of x to $\hat{A}$ or holding level some incorrect property defined as $\hat{A}$.

By executing the Zadeh's min-max method, complement function, FS union, and intersection are defined. The *union* of 2 FSs $\hat{C}$ and $\hat{D}$ is a FS in X, represented by $\hat{C} \cup \hat{D}$, the level of membership are provided as $\mu_{\hat{C}\cup\hat{D}} = \mu_{\hat{C}}(x) \vee \mu_{\hat{D}}(x) = \max\{\mu_{\hat{C}}(x), \mu_{\hat{D}}(x)\}$ for every $x \in X$.

$$\hat{C} \cup \hat{D} = \{\left(x, \mu_{\hat{C}\cup\hat{D}}(x)\right): \mu_{\hat{C}\cup\hat{D}}(x) = \max\{\mu_{\hat{C}}(x), \mu_{\hat{D}}(x)\}, \forall x \in X\}.$$

D. Neutrosophic FS and the application for taking decision

The *intersection* of $\hat{C}$ and $\hat{D}$ is a FS at X, defined by $\hat{C} \cap \hat{D}$ that level of membership are $\mu_{\hat{C}\cap\hat{D}} = \mu_{\hat{C}}(x) \wedge \mu_{\hat{D}}(x) = \max\{\mu_{\hat{C}}(x), \mu_{\hat{D}}(x)\}$ for every $x \in X$. Thus

$$\hat{C} \cap \hat{D} = \{\left(x, \mu_{\hat{C}\cap\hat{D}}(x)\right): \mu_{\hat{C}\cap\hat{D}}(x) = \max\{\mu_{\hat{C}}(x), \mu_{\hat{D}}(x)\}, \forall x \in X\}.$$

Assume $\hat{D}$ is a FS defining over X. Afterward its complement, $\hat{D}^c$, is represented in terms of membership degree as $\mu_{\hat{D}^c}(x) = 1 - \mu_{\hat{D}}(x)$ for every $x \in X$.

$$\hat{D}^c = \{(x, \mu_{\hat{D}^c}(x)): x \in X, \mu_{\hat{D}^c}(x) = 1 - \mu_{\hat{D}}(x)\}$$

This presents the NFS that the fuzzy membership degree of each component is compared with neutrosophic components such as truth, falsity, and indeterminacy membership levels. The integration of neutrosophic constituents to FS was needed to control the real-time data that take either unreliable or unpredictable. In different real-time problems, the level of membership of FS isn't completely ensured due to inaccurate and unreliable features of individual excellence. Therefore, it is more sensible to contain neutrosophic components to elect the membership level. The authors present the NFS. In other words, the level of membership of the neutrosophic components are defined by NFS.

Definition 2. Let Y is objects set and $\hat{A} = \{(y, \mu_{\hat{A}}(y)), \mu_{\hat{A}}(y) \in [0,1], y \in Y\}$ be a FS. Then, a NFS A in Y is represented by $A = \{y, \mu_A(y), T_A(y,\mu), I_A(y,\mu), F_A(y,\mu)\}, y \in Y$, each membership rate is indicated by falsity, indeterminacy, and truth membership function are defined as $T_A(y,\mu)$, $I_A(y,\mu)$, and $F_A(y,\mu)$. Moreover T_A, I_A and F_A take the real standard or nonstandard subsets of $]0^-, 1^+[$ T_A:$Y \rightarrow]0^-, 1^+[$, I_A: $Y \rightarrow]0^-, 1^+[$, and F_A: $Y \rightarrow]0^-, 1^+[$. Without restriction, the sum of T_A, I_A, and F_A. So, $0^- \leq supT_A + \sup I_A + \sup F_A \leq 3^+$. To set $\in Y$, $\{\mu_A(y), T_A(y), I_A(y), F_A(y)\}$, i.e., in simple procedure, $\{\mu_A, T_A, I_A, F_A\}$ is called as neutrosophic fuzzy number (NFN).

Besides T_A, I_A and F_A defines true nonstandard and standard subsets of$]0^-, 1^+[$, it is hard to execute NFS in engineering and scientific utilizes. It offers the single valued NFS (SVNFS) as further discussion.

Definition 3. Let use Y is object set of and $\hat{S} = \{(y, \mu_{\hat{S}}(y)), \mu_{\hat{S}}(y) \in [0,1], y \in Y\}$ be a FS. Afterward, the SVNFS S in Y is signified stated by $S = \{y, \mu_S(y)$, $T_S(y,\mu)$, $I_S(y,\mu)$, $F_S(y,\mu)\}, y \in Y$, in which $T_S(y,\mu)$, $I_S(y,\mu)$, $F_S(y,\mu) \in [0,1]$ and $0 \leq T_S(y,\mu) + I_S(y,\mu) + F_S(y,\mu) \leq 3$.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

4. The Proposed Method

In this paper, we have developed a new AOA-EFNSC approach for accurate intrusion detection and classification. The purpose of the AOA-EFNSC method is to recognize the presence of intrusions effectually. Fig. 1 depicts the entire workflow of the AOA-EFNSC system.

A. Data preprocessing

In a machine learning study, conducting exploratory data analysis and observing the data are essential to ensure that the dataset is well-suited for classification. These steps also play a crucial role in reducing the complexity and error rate of the classification model. This paper utilizes the UNSW and AIMD datasets, which undergo three pre-processing steps. These steps comprise encoding and normalization, sampling using k-means, and class oversampling using SMOTE. The following sections describe each step-in detail.

i. Min-Max Normalization

At the primary level, the AOA-EFNSC model, min-max scalar is applied to standardize the input data. Min-Max Scaling, better known as Min-Max normalization, it is a data pre-processing algorithm most frequently used in ML and statistics algorithms [22]. It includes converting arithmetical data features to a certain range, usually ranges within [0,1]. The process can be obtained by dividing the range (the variance among the minimum and maximum values) and subtracting the least value from the data point. This normalization technique is useful for ensuring that each feature contributes equally to the analyses, which prevents the big impact of variables on a large scale. Min-max scaling is increasingly being used to standardize data, which makes it suitable for algorithms that are sensitive to the scale of input features, ultimately improving the performance and convergence of ML techniques over different datasets.

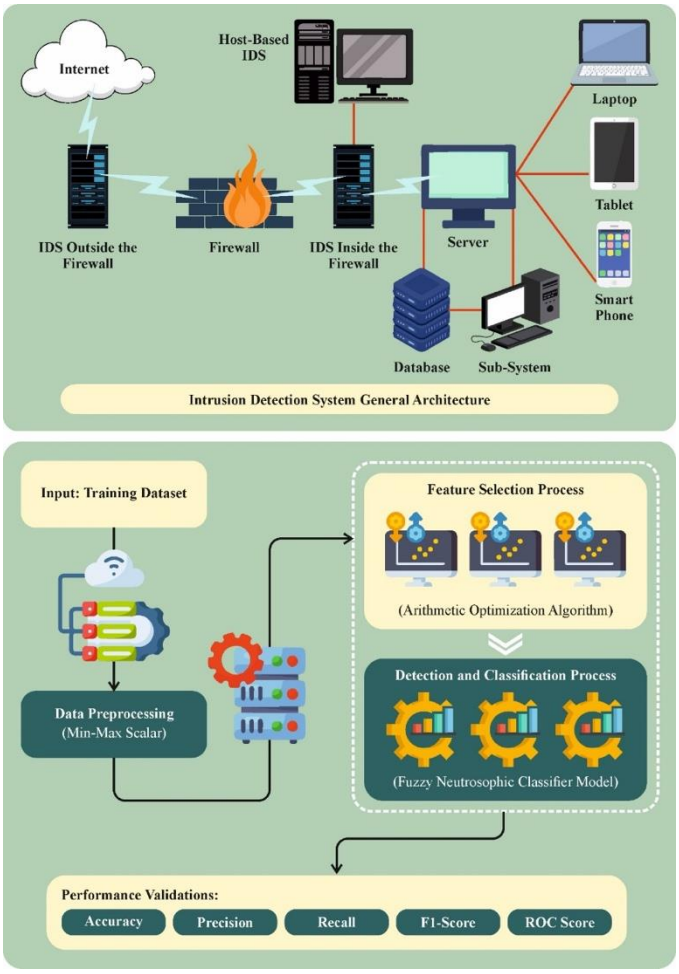

Figure 1: Overall flow of AOA-EFNSC technique

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

ii. Dataset sampling using k-means

Training Machine Learning Algorithms (MLA) on large network datasets can be impractical due to the time and computational resources required, especially when fine-tuning hyperparameters, which often involves training the MLA multiple times. To enhance training efficiency, sampling is commonly used to reduce the dataset size. This approach involves selecting a subset of the dataset to make training more manageable [39], [40]. In the proposed intrusion detection model, a cluster sampling method based on the k-means clustering procedure is used to obtain a good dataset subset. This method involves grouping the initial dataset instances into clusters and selecting a fraction of the dataset from each cluster to form the dataset subset [39]. Unlike random sampling, where instances are selected randomly with equal probability, clustering-based sampling can produce a better dataset subset by removing redundant instances.

Among clustering algorithms, k-means is widely used for dataset subset selection due to its simplicity, computational efficiency, and ability to produce meaningful clusters [40]. The k-means algorithm divides the data into clusters based on distance metrics such as Euclidean, Mahalanobis, or Manhattan distances [41], [42]. Since instances within the same cluster are similar, selecting instances from different clusters can significantly reduce the dataset size without losing important information. The primary objective of k-means is to minimize the sum of squared distances between dataset instances and their respective centroids, as shown in Eq. (10).

$$\sum_{i=0}^{m_p} \min_{c_j \in M_p} \left(y_i - c_j\right)^2 \tag{10}$$

In the equation, $(y_1, y_2, \ldots, y_m)$ represents the dataset instance matrix; c_j is the center of cluster M_p; and m_p is the number of instances in cluster M_p. The algorithm has a time complexity of $O(mpt)$, where m is the total number of instances in the dataset, p is the number of clusters, and t is the algorithm's stopping iteration [39]. After applying the k-means algorithm to divide the datasets into clusters, 10% of the instances in each cluster are selected using random sampling. The selected subsets from each cluster are then combined to form the final subset of the original dataset used in this study. The choice of 10% is based on resource constraints.

iii. Class imbalance handling

After normalizing and sampling the datasets, the study addresses class imbalances commonly found in network traffic flow datasets. These imbalances arise because genuine traffic flow instances significantly outnumber attack traffic flow instances in real-world scenarios. This imbalance can lead to biased models and poor detection rates [44]. Class imbalance challenges are typically mitigated using resampling strategies such as random sampling and Synthetic Minority Over-sampling Technique (SMOTE), which generate new instances to balance the dataset [44]-[45]. Unlike random sampling, which simply duplicates instances and can lead to overfitting, SMOTE [46] generates high-quality synthetic instances based on the k Nearest Neighbors (KNN) approach. Therefore, SMOTE is selected in this study to effectively address the class imbalance problem, resulting in high-quality minority class examples. Equation (11) is used to generate the new instances in the minority classes.

For instance, if X is an instance in the smaller class and Y is an instance selected randomly from the neighbours of X, an artificial instance Z is generated using Eq. (11). The balanced datasets using SMOTE represents the final dataset used for feature selection and subsequently for building the proposed intrusion detection model.

$$Y_m = X + r^*(\mathrm{Y} - X), i = 1,2,3, \ldots, k \tag{11}$$

B. Feature Selection

Feature selection plays a crucial role in developing network intrusion detection models by selecting important attributes and eliminating irrelevant and redundant ones. It helps reduce the complexity and difficulty of the model. In this study, we select features using the proposed Binary Arithmetic Optimization Algorithm (AOA) optimization algorithm as the search strategy and the EFNSC as the learning algorithm in the wrapper feature selection method, following the preprocessing procedure. The goal of our study is to decrease the number of features while ensuring the classification accuracy of the machine learning model. To guide the BAOA algorithm search, we use the fitness function shown in Eq. (12).

$$Fitness = \alpha * ErrorRate + (1 - \alpha) * \frac{\#SF}{\#All\_F} \tag{12}$$

Whereas ErrorRate denotes the error rate of classifier utilizing the nominated feature. ErrorRate is intended as the ratio of improper categorized to the integer of classification prepared, stated as a value amongst 0 and 1. (ErrorRate

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

is the complement of the classifier accuracy), $\#SF$ is the number of nominated features and $\#All\_F$ designates the total amount of attributes in the original database. α is employed to switch the significance of classification excellence and subset length. In our tests, α is set to 0.9.

C. Intrusion Detection using FNSC

For intrusion detection, the AOA-EFNSC technique uses the FNSC technique for the recognition and identification of the intrusions. Fuzzy logic (FL) was developed by Prof. L.A. Zadeh [24]. However, by weak acceptance firstly, gradually it is presented as one of the significant soft calculating methods to perfect uncertainty. Real data is filled with gaps, inconsistent and uncertain information. The uncertainty can meet in diverse methods such as in the result of tossing a coin; whether it is a tail or head is an instance of standard bivalence whereas uncertainty fades on the conclusion of the result. The main work is devoted to delivering enlargement to the generally utilized fuzzy classifier in the method of the neutrosophic classifier and employs FL. Therefore, this part provides you with brief facts about a fuzzy classifier and FL in its common method. Prof. L. Zadeh developed the area of logic by presenting a new FL, where every element has a grade of membership in a fuzzy set.

Definition 1. Fuzzy set and membership function

Assume that Z is an assortment of objects that are signified by z, then a fuzzy set A in Z is definite as a set of well-ordered:

$$A = \{(z, \mu_A(z) | z \in Z\} \tag{12}$$

$\mu_A(z)$ denotes the membership function (MF) of z. It maps every element of Z to a constant membership value among (0,1). Also, it has the condition of permitting linguistic variables whose truth value may differ amongst 0 and 1; in reverse to dual values of traditional logic.

Then the start of the fuzzy set model, the classifier area is a vital theoretic and real-world fuzzy application area. Crisp classes signify an impractical simplification of realism that the fuzzy technique seems to control very effortlessly. A fuzzy classifier uses C a set of classes. Then, the issue is determined for each object z below concern, $z \in Z$, the degree $\mu_C(z)$ to object z that fits to class $c \in C$.

So, an MF $\mu_C(z): Z \to [0,1]$ is definite for every class $c \in C$.

A fuzzy classifier employs familiar information about the issue area for classification. It is handled by generating fuzzy-type ML that changes accurate computable parameters to group membership that are utilized for fuzzy classifier. MF denotes to corresponding intervals of feature value. In an n-dimensional actual space R^n, assume that z be a vector and $C = \{c_1, c_2, \dots, c_c\}$ is a set of class labels. Bezdek et al. have a definite fuzzy and crisp classifier. A crisp classifier is as follows:

$$O_c: R^n \to C \tag{13}$$

A fuzzy classifier utilizes fuzzy sets either at the time of training or its process. It employs a fuzzy if-then inference method that produces class labels for z.

$$O_F: R^n \to [0,1]^c \tag{14}$$

So, rather than allocating a class label from C, O_F gives $z \in R^n$ to a soft class label with grades of membership in every class.

$$R^n \to \mu_C(z) \forall z \in R^n \; and \sum_{i=1}^{c} \mu_i(z) = 1 \tag{15}$$

The outcome is signified by $O_F = \{(z, \mu_C(z)) | z \in R^n\}$.

The next section explains you about neutrosophic logic (NL). Currently, NL is dependent upon the analysis of non-standard. It has been presented to signify mathematical techniques of vagueness, uncertainty, imprecision, ambiguity, inconsistency, contradiction, redundancy, and incompleteness. NL is a logic where the plan is assessed to have the ratio of indeterminacy in a subset I, the ratio of truth in a subset T, and the ratio of falsity in a subset F, whereas T, I, F denotes the non-standard or standard real subsets of $]^-0, 1^+[$:

with

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

$$\sup T = t\_\sup, infT = t\_\inf \quad (16)$$

$$sup\ I = i\_sup\ , infI = i\_inf \quad (17)$$

$$sup\ F = f\_sup\ , infF = f\_\inf \quad (18)$$

and

$$n\_sup = t\_sup + i\_sup + f\_sup \quad (19)$$

$$n_{inf} = t\_inf + i\_inf + f\_inf\ . \quad (20)$$

The T, I, and F are not certain intervals but might be real sub-unitary subsets: separate or nonstop; single element, limited, or infinite; union or connection of many subsets; etc. We employ a subset of truth, indeterminacy, or falsity in its place of an integer only, because numerous cases are not capable of precisely defining the ratios but estimate them. Entire factors are specified by NL, which are extremely essential to human thought, as it is unusual that we are inclined to complete in certain surroundings, the roughness of human methods might be owing to the limitation of data that human obtains from the exterior world. Indeterminacy is the area of ignorance of a proposition's value, among falsehood and truth, where certainly neutrosophic modules fit in the demonstrating of imitation of human brain cognitive.

Definition 2. Neutrosophic set: Assume that Z is a space of points by a generic element in Z represented by z.

A neutrosophic set A in Z is categorized by MFs of truth T_A, an indeterminacy- I_A and a falsity F_A. $T_A(z)$, $I_A(z)$ and $F(z)$ denotes the real non-standard or standard subsets of $]^-0, 1^+[$. That is

$$T_A: Z \rightarrow]^-0, 1^+[\quad (21)$$

$$I_A: Z \rightarrow]^-0, 1^+[\quad (22)$$

$$F_A: Z \rightarrow]^-0, 1^+[\quad (23)$$

It has no constraint on the calculation of $T_A(z)$, $I(z)$ and $F_A(z)$, so

$$-0 = \sup T_A(z) + \sup I_A(z) + \sup F_A(z) = 3^+ \quad (24)$$

This classifier is nothing but an algorithm that forecasts the class labels on the foundation of the object descriptor. The generally utilized classifier in the easy-calculating area is a fuzzy classifier. It employed fuzzy sets or logic during its training or process. This paper suggests fuzzy classifier because it is a neutrosophic classifier that will employ NL because it is a superset of fuzzy logic.

Definition 3. Neutrosophic classifier: It employs NL values and sets for the identification. It integrates an easy and neutrosophic rule-based technique such as IF X and Y THEN Z, for resolving the issue rather than trying to perfect a method arithmetically parallel to the fuzzy classifier. Assume let z be a vector in an n-dimensional realspace R^n and let $C = \{c_1, c_2, \dots, c_c\}$ is a class label. It is definite as:

$$O_N: R^n \rightarrow \{T_C(z), I_C(z), F_C(z) | x \in R^n\} \quad (25)$$

The output of O_N is signified as

$$O_N = \{(z, [T_C(z), I_C(z), F_C(z)]) | z \in R^n\} \quad (26)$$

where

$$[T_C(z)] = \begin{bmatrix} t_{c_1}(z) \\ t_{c_2}(z) \\ \cdot \\ \cdot \\ t_{c_C}(z) \end{bmatrix}, [I_C(z)] = \begin{bmatrix} i_{c_1}(z) \\ i_{c_2}(z) \\ \cdot \\ \cdot \\ i_{c_C}(z) \end{bmatrix} \quad (27)$$

and

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

$$[F_C(z)] = \begin{bmatrix} f_{c_1}(z) \\ f_{c_2}(z) \\ \cdot \\ \cdot \\ f_{c_c}(z) \end{bmatrix} \tag{28}$$

T, I, and F are independent of each other and have no constraint on the amount of $T_C(z)$, $I_C(z)$ and $F_C(z)$, so

$$-0 \leq T_C(z) + I_C(z) + F_C(z) = 3^+ \tag{29}$$

The non-standard unit range $]^-0, 1^+[$ is just employed for logical uses, particularly when difference is needed among relative and absolute indeterminacy/falsehood/truth/. But for practical uses of NL and set, the area of description and range of T, I, and F can be controlled to the usual standard unit range of [0 and1] that is very simple to utilize.

D. Evaluation metrics

In assessing the network intrusion detection model, we employed five evaluation metrics commonly used in evaluating similar research in intrusion detection systems, as seen in studies by [46]-[48].

- **Accuracy:** Is the ratio of the number of intrusions (T^{Positive}) and normal activities (T^{Negative}) that are identified effectively to the number of the instances in the dataset as depicted in Eq.(30)

$$\text{Accuracy} = \frac{T^{\text{Positive}} + T^{\text{Negative}}}{T^{\text{Positive}} + F^{\text{Positive}} + T^{\text{Negative}} + F^{\text{Positive}}} \tag{30}$$

- **Recall:** Is the proportion of the number of intrusions that are identified effectively (i. e. True positive (T^{positive})) to the sum of the amount of intrusions that are recognized as intrusion (T^{positive}) and the amount of normal activities that are recognized as normal (i.e. True negative (F^{Negative}) as depicted in Eq.(31).

$$\text{Recall} = \frac{T^{\text{positive}}}{T^{\text{positive}} + F^{\text{Negative}}} \tag{31}$$

- **Precision:** Is the proportion of the number of intrusions (T^{positive}) that are identified to the total amount of intrusion (T^{positive}) and normal (F^{positive}) activities identified that as depicted in Eq.(32).

$$\text{Precision} = \frac{T^{\text{positive}}}{T^{\text{positive}} + F^{\text{positive}}} \tag{32}$$

- **F-measure:** Define as the harmonic mean of recall and precision metrics which is depicted in Eq.(33).

$$F - \text{measure} = \frac{2^* \text{Preciion} * \text{Recall}}{\text{Precision} + \text{Recall}} \tag{33}$$

5. Experimental Validation

In this section, various tests and experiments were conducted to assess the effectiveness of the proposed network intrusion detection model. The hardware and software used are detailed below.

A. Experimental Setup

The experiments were conducted on a system with an Intel® Pentium® CPU 10750 @ 2.60, 16.00 GB of RAM, and a 64-bit Operating System. The tests were performed using the Python programming language in Jupyter Notebook.

B. Result discussion

The performance analysis of the AOA-EFNSC approach takes place using UNSW-NB15 and AWID datasets. Table 1 demonstrates the details of the UNSW_NB15 dataset, which contains 2000 samples under two classes.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

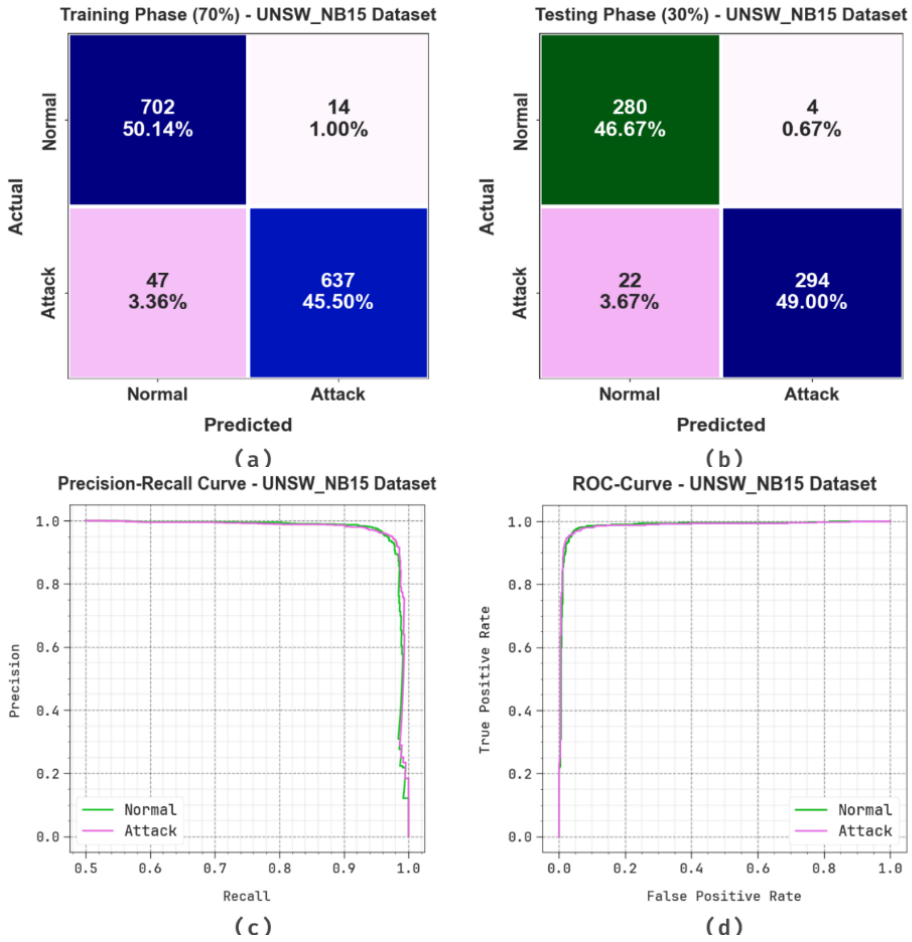

Figure 3: UNSW_NB15 Dataset (a-b) Confusion matrices and (c-d) PR and ROC curves

Table 1: Details on UNSW_NB15 Dataset

UNSW_NB15 Dataset	
Class	No. of Samples
Normal	1000
Attack	1000
Total Samples	2000

Fig. 3 establishes the classifier outcomes of the AOA-EFNSC model below the UNSW_NB15 dataset. Figs. 3a-3b portrays the confusion matrices presented by the AOA-EFNSC technique on 70:30 of TRAPH/TESPH. The figure indicated that the AOA-EFNSC method has familiar and classified all 2 class labels exactly. Similarly, Fig. 3c proves the PR analysis of the AOA-EFNSC technique. The figure specified that the AOA-EFNSC technique has attained maximum PR performance under all classes. Lastly, Fig. 3d exemplifies the ROC study of the AOA-EFNSC approach. The figure represented that the AOA-EFNSC technique has resulted in proficient outcomes with the greatest ROC values below separate class labels.

Table 2 represents the detection results of the AOA-EFNSC technique on the UNSW_NB15 dataset. The results imply that the AOA-EFNSC technique reaches optimal normal and attack recognition. With 70%TRAPH, the AOA-EFNSC technique gains an average $accu_y$ of 95.59%, $prec_n$ of 95.79%, $reca_l$ of 95.59%, $F1_{score}$ of 95.63%, and ROC_{score} of 95.59%. Additionally, with 30%TESPH, the AOA-EFNSC method attains average $accu_y$ of 95.81%, $prec_n$ of 95.69%, $reca_l$ of 95.81%, $F1_{score}$ of 95.66%, and ROC_{score} of 95.81%.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

Table 2: Detection outcome of AOA-EFNSC technique on UNSW_NB15 dataset

UNSW_NB15 Dataset					
Classes	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	ROC_{Score}
TRAPH (70%)					
Normal	98.04	93.72	98.04	95.84	95.59
Attack	93.13	97.85	93.13	95.43	95.59
Average	95.59	95.79	95.59	95.63	95.59
TESPH (30%)					
Normal	98.59	92.72	98.59	95.56	95.81
Attack	93.04	98.66	93.04	95.77	95.81
Average	95.81	95.69	95.81	95.66	95.81

Table 3: Details on AWID Dataset

AWID Dataset	
Class	No. of Samples
Normal	1000
Attack	1000
Total Samples	2000

Table 3 determines the details of AWID dataset, includes 2000 samples below two classes. Fig. 4 determines the classifier outcomes of the AOA-EFNSC approach below the AWID dataset. Figs. 4a-4b portrays the confusion matrices presented by the AOA-EFNSC technique on 70:30 of TRAPH/TESPH.

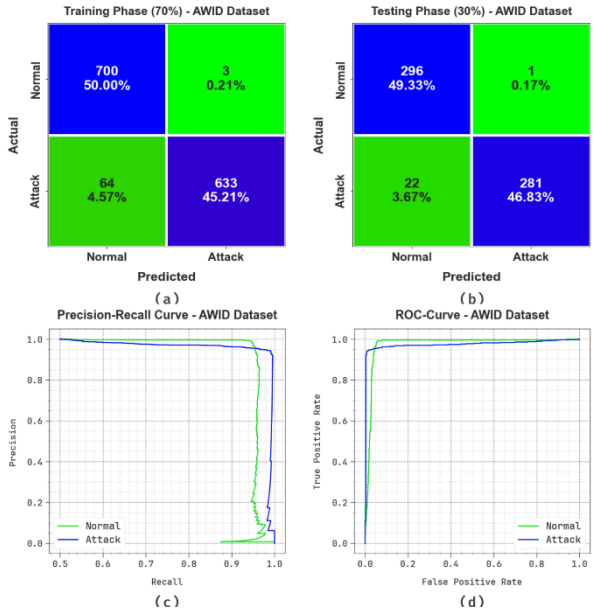

Figure 4: AWID Dataset (a-b) Confusion matrices and (c-d) PR and ROC curves

Figure 4 shows that the AOA-EFNSC system has well-known and classified all 2 class labels accurately. Similarly, Fig. 4c establishes the PR study of the AOA-EFNSC approach. The figure described that the AOA-EFNSC system has increased the greatest performance of PR under all classes. Lastly, Fig. 4d clarifies the ROC study of the AOA-EFNSC method. The figure defined that the AOA-EFNSC methodology has resulted in capable outcomes with the maximum ROC values below separate class labels.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

Table 4 signifies the recognition results of the AOA-EFNSC method on the AWID dataset. The outcomes indicate that the AOA-EFNSC system extents optimum normal and attack detection. With 70%TRAPH, the AOA-EFNSC method attains average $accu_y$ of 95.20%, $prec_n$ of 95.58%, $reca_l$ of 95.20%, $F1_{score}$ of 95.20%, and ROC_{score} of 95.20%. Moreover, with 30%TESPH, the AOA-EFNSC procedure attains average $accu_y$ of 96.20%, $prec_n$ of 96.36%, $reca_l$ of 96.20%, $F1_{score}$ of 96.16%, and ROC_{score} of 96.20%.

Table 4: Detection outcome of AOA-EFNSC technique on AWID dataset

AWID Dataset					
Classes	$\boldsymbol{Accu_y}$	$\boldsymbol{Prec_n}$	$\boldsymbol{Reca_l}$	$\boldsymbol{F1_{Score}}$	$\boldsymbol{ROC_{Score}}$
TRAPH (70%)					
Normal	99.57	91.62	99.57	95.43	95.20
Attack	90.82	99.53	90.82	94.97	95.20
Average	95.20	95.58	95.20	95.20	95.20
TESPH (30%)					
Normal	99.66	93.08	99.66	96.26	96.20
Attack	92.74	99.65	92.74	96.07	96.20
Average	96.20	96.36	96.20	96.16	96.20

Table 5 and Fig. 5 illustrate the comparison results of the AOA-EFNSC technique [25]. The results indicate that the SVM, NB-Bagging, NB-Adaboost, GCNSE, and CNN-Adaboost techniques have shown worse performance. In the meantime, the BBAFS-DRL model has tried to exhibit reasonable performance. However, the AOA-EFNSC technique demonstrates superior performance with increased $accu_y$ of 96.20%, $prec_n$ of 96.36%, $reca_l$ of 96.20%, and $F1_{score}$ of 96.16%. Thus, the AOA-EFNSC technique can be applied for an enhanced intrusion recognition process.

Table 5: Comparative analysis of AOA-EFNSC technique with recent approaches

Methods	Accuracy	Precision	Recall	F1-Score
AOA-EFNSC	96.20	96.36	96.20	96.16
BBAFS-DRL	95.04	95.22	95.06	95.04
SVM Model	75.91	78.72	76.24	77.76
NB-Bagging Algorithm	70.01	69.53	72.81	70.93
NB-Adaboost Algorithm	71.34	74.44	73.13	74.07
GCNSE Model	80.17	80.01	81.28	80.82
CNN-Adaboost Algorithm	74.16	69.28	71.53	68.16

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

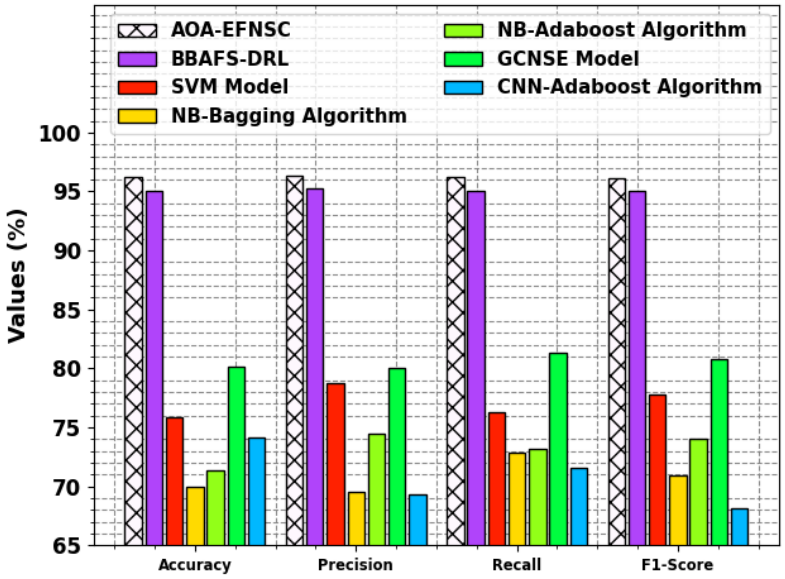

Figure 5: Comparative analysis of AOA-EFNSC technique with recent approaches

6. Conclusion

In this study, we have developed a novel AOA-EFNSC system for accurate intrusion detection and classification. The purpose of the AOA-EFNSC method is to recognize the presence of intrusions effectually. In the AOA-EFNSC technique, a min-max scalar is applied to normalize the input data. Besides, the AOA-EFNSC technique employs AOA based FS technique to select a subset of feature. For intrusion detection, the AOA-EFNSC technique uses the FNSC technique for the recognition and classification of the intrusions. An experimentations were involved to validate the superior performance of AOA-EFNSC technique. The experimental values pointed out that the AOA-EFNSC model gains enhanced detection results over other models.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Om Prakash, P.G., Maram, B., Nalinipriya, G. and Cristin, R., 2021. Harmony search Hawks optimization-based Deep reinforcement learning for intrusion detection in IoT using nonnegative matrix factorization. International Journal of Wavelets, Multiresolution and Information Processing, 19(04), p.2050093.

[2] Hsu, Y.F. and Matsuoka, M., 2020, November. A deep reinforcement learning approach for anomaly network intrusion detection system. In 2020 IEEE 9th International Conference on Cloud Networking (CloudNet) (pp. 1-6). IEEE.

[3] Dang, Q.V. and Vo, T.H., 2022. Reinforcement learning for the problem of detecting intrusion in a computer system. In Proceedings of Sixth International Congress on Information and Communication Technology (pp. 755-762). Springer, Singapore.

[4] Anil Audumbar Pise, Saurabh Singh, Hemachandran K., Shraddhesh Gadilkar, Zakka Benisemeni Esther, Ganesh Shivaji Pise, Jude Imuede, Investigating Recent Advances In Coded Diffraction Patterns using Deep Learning, Journal of International Journal of Wireless and Ad Hoc Communication, Vol. 7 , No. 1 , (2023) : 62-71 (Doi : https://doi.org/10.54216/IJWAC.070106)

[5] Venturi, A., Apruzzese, G., Andreolini, M., Colajanni, M. and Marchetti, M., 2021. Drelab-deep reinforcement learning adversarial botnet: A benchmark dataset for adversarial attacks against botnet intrusion detection systems. Data in Brief, 34, p.106631.

[6] Priya, S. and PradeepMohankumar, K., 2021, December. Intelligent Outlier Detection with Optimal Deep Reinforcement Learning Model for Intrusion Detection. In 2021 4th International Conference on Computing and Communications Technologies (ICCCT) (pp. 336-341). IEEE.

[7] Alavizadeh, H., Alavizadeh, H. and Jang-Jaccard, J., 2022. Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection. Computers, 11(3), p.41.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

[8] Gupta, G.P., 2022. Intrusion Detection Framework Using an Improved Deep Reinforcement Learning Technique for IoT Network. In Soft Computing for Security Applications (pp. 765-779). Springer, Singapore.
[9] Alawsi, A.S.S. and Kurnaz, S., 2022. Quality of service system that is self-updating by intrusion detection systems using reinforcement learning. Applied Nanoscience, pp.1-8.
[10] Bouhamed, O., Bouachir, O., Aloqaily, M. and Al Ridhawi, I., 2021, May. Lightweight ids for uav networks: A periodic deep reinforcement learning-based approach. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 1032-1037). IEEE.
[11] Park, S.B., Jo, H.J. and Lee, D.H., 2023. G-idcs: Graph-based intrusion detection and classification system for can protocol. *IEEE Access*.
[12] Fayed, N.S., Elmogy, M.M., Atwan, A. and El-Daydamony, E., 2022. Efficient Occupancy Detection System Based on Neutrosophic Weighted Sensors Data Fusion. IEEE Access, 10, pp.13400-13427.
[13] Hassan, G.M., Gumaei, A., Alanazi, A. and Alzanin, S.M., 2023. A Network Intrusion Detection Approach Using Extreme Gradient Boosting with Max-Depth Optimization and Feature Selection. International Journal of Interactive Mobile Technologies, 17(15).
[14] Zainudin, A., Akter, R., Kim, D.S. and Lee, J.M., 2023. Federated Learning Inspired Low-Complexity Intrusion Detection and Classification Technique for SDN-Based Industrial CPS. *IEEE Transactions on Network and Service Management*.
[15] Prasad, M., Tripathi, S. and Dahal, K., 2023. A probability estimation-based feature reduction and Bayesian rough set approach for intrusion detection in mobile ad-hoc network. Applied Intelligence, 53(6), pp.7169-7185.
[16] Sajithra Varun, S. and Nagarajan, G., 2023. DeepAID: a design of smart animal intrusion detection and classification using deep hybrid neural networks. *Soft Computing*, pp.1-12.
[17] Abdelhafeez, A., Mohamed, H.K., Maher, A. and Khalil, N.A., 2023. A novel approach toward skin cancer classification through fused deep features and neutrosophic environment. Frontiers in Public Health, 11, p.1123581.
[18] Alshehri, M.D., 2023. An integrated AHP MCDM based Type-2 Neutrosophic Model for Assessing the Effect of Security in Fog-based IoT Framework. *International Journal of Neutrosophic Science (IJNS)*, *20*(2).
[19] Chinnasamy, V. and Rajasekaran, S., 2023. Multi-Valued Neutrosophic Convolutional LSTM for Intrusion Detection. *International Journal of Intelligent Engineering & Systems*, *16*(5).
[20] Mirza, O.M. and Samak, A.H., 2024. Neutrosophic Fuzzy Logic-Based Hybrid CNN-LSTM for Accurate Chest X-ray Classification in COVID-19 Prediction. *Appl. Math*, *18*(1), pp.139-152.
[21] Dias, T.F., Vitorino, J., Fonseca, T., Praça, I., Maia, E. and Viamonte, M.J., 2023, September. Unravelling Network-Based Intrusion Detection: A Neutrosophic Rule Mining and Optimization Framework. In *European Symposium on Research in Computer Security* (pp. 59-75). Cham: Springer Nature Switzerland.
[22] Henderi, H., Wahyuningsih, T. and Rahwanto, E., 2021. Comparison of Min-Max normalization and Z-Score Normalization in the K-nearest neighbor (kNN) Algorithm to Test the Accuracy of Types of Breast Cancer. International Journal of Informatics and Information Systems, 4(1), pp.13-20.
[23] Dhal, K.G., Sasmal, B., Das, A., Ray, S. and Rai, R., 2023. A comprehensive survey on arithmetic optimization algorithm. Archives of Computational Methods in Engineering, 30(5), pp.3379-3404.
[24] A. A. Salama, H. A. Elagamy, On Neutrosophic Fuzzy Ideal Concepts, Journal of International Journal of Neutrosophic Science, Vol. 14 , No. 2 , (2021) : 98-103 (Doi : https://doi.org/10.54216/IJNS.140203)
[25] Priya, S. and Kumar, K., 2023. Binary bat algorithm based feature selection with deep reinforcement learning technique for intrusion detection system. Soft Computing, pp.1-12.
[26] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897.
[27] Bakro, M., Kumar, R. R., Alabrah, A., Ashraf, Z., Ahmed, M. N., Shameem, M., & Abdelsalam, A. (2023). An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier. IEEE Access.
[28] Alkanhel, R., El-kenawy, E. S. M., Abdelhamid, A. A., Ibrahim, A., Alohali, M. A., Abotaleb, M., & Khafaga, D. S. (2023). Network Intrusion Detection Based on Feature Selection and Hybrid Metaheuristic Optimization. Computers, Materials & Continua, 74(2).
[29] Hassan, I. H., Abdullahi, M., Aliyu, M. M., Yusuf, S. A., & Abdulrahim, A. (2022). An improved binary manta ray foraging optimization algorithm based feature selection and random forest classifier for network intrusion detection. Intelligent Systems with Applications, 16, 200114.
[30] Kareem, S. S., Mostafa, R. R., Hashim, F. A., & El-Bakry, H. M. (2022). An effective feature selection model using hybrid metaheuristic algorithms for iot intrusion detection. Sensors, 22(4), 1396.
[31] Subramani, S., & Selvi, M. (2023). Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks. Optik, 273, 170419.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024

[32] Kamalesh, S., & Muthukrishnan, A. (2023). Optimized dictionary-based sparse regression learning for health care monitoring in IoT-based context-aware architecture. IETE Journal of Research, 1-16.
[33] Ebrahimpour, M. K., & Eftekhari, M. (2017). Ensemble of feature selection methods: A hesitant fuzzy sets approach. Applied Soft Computing, 50, 300-312.
[34] Zarshenas, A., & Suzuki, K. (2016). Binary coordinate ascent: An efficient optimization technique for feature subset selection for machine learning. Knowledge-Based Systems, 110, 191-201.
[35] Han, C., Zhou, G., & Zhou, Y. (2019). Binary symbiotic organism search algorithm for feature selection and analysis. IEEE Access, 7, 166833-166859.
[36] Islam, M. J., Li, X., & Mei, Y. (2017). A time-varying transfer function for balancing the exploration and exploitation ability of a binary PSO. Applied Soft Computing, 59, 182-196.
[37] Yi, J. H., Wang, J., & Wang, G. G. (2016). Improved probabilistic neural networks with self-adaptive strategies for transformer fault diagnosis problem. Advances in Mechanical Engineering, 8(1), 1687814015624832.
[38] Mirjalili, S., & Lewis, A. (2013). S-shaped versus V-shaped transfer functions for binary particle swarm optimization. Swarm and Evolutionary Computation, 9, 1-14.
[39] Faraoun, K. M., & Boukelif, A. (2006). Neural networks learning improvement using the K-means clustering algorithm to detect network intrusions. INFOCOMP Journal of Computer Science, 5(3), 28-36.
[40] Yang, L., Moubayed, A., & Shami, A. (2021). MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles. IEEE Internet of Things Journal, 9(1), 616-632.
[41] Na, S., Xumin, L., & Yong, G. (2010, April). Research on k-means clustering algorithm: An improved k-means clustering algorithm. In 2010 Third International Symposium on intelligent information technology and security informatics (pp. 63-67). Ieee.
[42] Moubayed, A., Injadat, M., Shami, A., & Lutfiyya, H. (2018, December). Dns typo-squatting domain detection: A data analytics & machine learning based approach. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.
[43] Moubayed, A., Injadat, M., Shami, A., & Lutfiyya, H. (2020). Student engagement level in an e-learning environment: Clustering using k-means. American Journal of Distance Education, 34(2), 137-156.
[44] Chen, Z., Yan, Q., Han, H., Wang, S., Peng, L., Wang, L., & Yang, B. (2018). Machine learning based mobile malware detection using highly imbalanced network traffic. Information Sciences, 433, 346-364.
[45] Onah, J. O., Abdullahi, M., Hassan, I. H., & Al-Ghusham, A. (2021). Genetic Algorithm based feature selection and Naïve Bayes for anomaly detection in fog computing environment. Machine Learning with applications, 6, 100156.
[46] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: synthetic minority over-sampling technique. Journal of artificial intelligence research, 16, 321-357.
[47] Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University-Computer and Information Sciences, 31(4), 541-553.
[48] Talita, A. S., Nataza, O. S., & Rustam, Z. (2021, February). Naïve bayes classifier and particle swarm optimization feature selection method for classifying intrusion detection system dataset. In Journal of physics: conference series (Vol. 1752, No. 1, p. 012021). IOP Publishing.

DOI: https://doi.org/10.54216/IJNS.240415
Received: November 07, 2023 Revised: March 23, 2024 Accepted: June 01, 2024