Enhancing Network Security using Possibility Neutrosophic Hypersoft Set for Cyberattack Detection

Mohammed Abdullah Al-Hagery[1,*], Abdalla I. Abdalla Musa[1]

[1]Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia
Emails: hajry@qu.edu.sa; ab.musa@qu.edu.sa

Abstract

Network security is any endeavor intended to defend the integrity and usability of the data and network. Fast development in network technology and the scope and amount of information transported on a network is gradually growing. Based on these situations, the complexity and density of cyber-attacks and threats are also increasing. The constantly expanding connectivity makes it more difficult for cyber-security specialists to monitor all the movements on the network. More complex and frequent cyber-attack makes anomaly identification and detection in network events challenging. Machine learning (ML) provides different techniques and tools to automate cyber-attack detection and for prompt prognosis and analysis of attack types. The model of a neutrosophic hypersoft set (NHSS) is a combination of a neutrosophic set with a hypersoft set. It is a useful structure to handle multi-objective problems and multi-attributes with disjoint attributable values. This study derives the Possibility Neutrosophic Hypersoft Set for Cyberattack Detection (pNHSS-CAD) technique to improve network security. The pNHSS-CAD method has its formation in feature selection with the Whale Optimization Algorithm (WOA), which successfully recognizes the important features from the data, thus improving processing speed and reducing dimensionality. Following feature selection, the pNHs-set classifier is employed for the robust detection and identification of cyber-attacks, which leverages the power of the neutrosophic set to deal with ambiguity and uncertainty in the information. The Firefly (FF) technique is applied for hyperparameter fine-tuning, which ensures the model operates at maximum effectiveness to enhance the performance of the classification. This wide-ranging method leads to a very efficient cyberattack recognition method, which can able to accurately mitigate and identify risks in the real world

Keywords: Network security; Artificial intelligence; Risk factors; Machine learning; Cyberattacks

1. Introduction

To define the characteristics of people, commonly utilize appropriate values when they come through decision-making issues [1]. In contrast, it is detected that in a situation of decision-making, we face numerous difficult and variable issues [2]. While for fuzzy languages, the decision-makers will take aid from the linguistic assessments. For example, the assessment values were signified by the usage of languages like V.good, outstanding, and good by the decision makers [3]. At first, the soft set (SS) model was employed as a normal accurate mean to derive through the complexity of uncertainty and hesitation. A similar model of the sentimental set is allowed from the parameterization insufficiency syndrome of the FS model, rough set model, and functional mathematics [4]. A neutrosophic set (NS) is a very great device to beat imperfect and unknown data intended. Also, it has appealed to numerous students that might provide the credibility of the assumed linguistic study value and set can provide qualitative analysis value [5]. SS is general to hypersoft set by re-modeling the task into a function of multi-attribute, NHSS (Neutrosophic Hyper Soft Set) is furthermore intended in his pioneer work.

As a developing technology invention, IoT has allowed the processing, assortment, and data communication in smart uses [6]. These new features have appealed to city designers and health specialists because IoT is attaining huge use in the systems for applications like smart cities and eHealth [7]. However, the development and complexity of strange cyberattacks have performers on the approval of these smart services. This originates that

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

the spread and diversity of IoT applications create the safety of IoT [8]. Furthermore, attack recognitions in IoT are very dissimilar from the present devices due to the special service desires of IoT such as resource limitations, lower latency, scalability, distribution, and flexibility [9]. This indicates that standalone neither cloud attack recognition resolves the safety issues of IoT. The dynamic and constant nature of cyberattacks requires the manufacture of a structure with well-considered significance [10]. There is always a risk that certain incursions might be more hazardous when compared to others and will have a main effect on processes [11]. So, the energetic force is to generate a method that can distinguish among numerous threat levels so that an effective and targeted response may be prepared [12]. By placing the most severe dangers, their impact on manufacturing processes is both prohibited and diminished [13]. A predictive structure is also proposed to begin an active protection mechanism. The main objective is to predict and stop probable dangers rather than replying to cracks after they occur [14]. Over the study of historical data and the present behavior of the network, predictive methods are capable of recognizing patterns, which specify probable dangers before them visible [15].

This study derives the Possibility Neutrosophic Hypersoft Set for Cyberattack Detection (pNHSS-CAD) technique to improve network security. The pNHSS-CAD method has its formation in feature selection with the Whale Optimization Algorithm (WOA), which successfully recognizes the important features from the data, thus improving processing speed and reducing dimensionality. Following feature selection, the pNHs-set classifier is employed for the robust detection and identification of cyber-attacks, which leverages the power of the neutrosophic set to deal with ambiguity and uncertainty in the information. The Firefly (FF) technique is applied for hyperparameter fine-tuning, which ensures the model operates at maximum effectiveness to enhance the performance of the classification. This wide-ranging method leads to a very efficient cyberattack recognition method, which can able to accurately mitigate and identify risks in the real world.

2. Literature Survey

Vaiyapuri et al. [16] introduce an Improved Reptile Search Optimizer with an Ensemble Deep Learning Cyber-security (IRSO-EDLCS) approach in the IIoT atmosphere. The proposed IRSO-EDLCS model accomplishes the IRSO technique-based feature selection (IRSO-FS) model. Additionally, the IRSO-EDLCS model achieves an ensemble of 3 DL methods. The modified gray wolf optimizer (MGWO) method is utilized for the hyperparameter tuning process. Ding et al. [17] propose an alternate DL technique namely DeepAK-IoT. The RSR block utilizes 5 residual blocks for extracting a feature symbol from the prior layer's outcome. The 4 convolutional layers are related parallelly with a skip connection in every block to evade exploding or vanishing gradients. Later, the 2nd block employs the removed spatial representation for learning a time-based representation. The last block concludes by classifying the input data.

In [18], an effectual DL-based technique is proposed for identifying network threats in SDN. This methodology encompasses enhanced ShuffleNetV2, a data augmentation generative adversarial network (DAGAN), and Xception models. Initially, DAGAN is utilized for increasing data samples and reducing class imbalance issues in the dataset. Later, the crucial factors are extracted using the Xception method. Lastly, intrusions are recognized and classified by implementing an enhanced ShuffleNetV2 model. Assiri and Ragab [19] introduce the Honey Badger Algorithm with an Optimum Hybrid Deep Belief Networks (HBA-OHDBN) model. This model utilized HBA for feature selection and for choosing an optimum feature set. The model also employed HDBN methodology for intrusion detection. Furthermore, the Dung Beetle Optimizer (DBO) approach is applied for altering the hyperparameter outputs of the HDBN method. Finally, the Blockchain (BC) technology is also utilized for enhancing network safety.

Hussain et al. [20] present a technique that employs the Deep Q-Network (DQN) model as it can learn to recognize challenges depending on network traffic data without relying on pre-determined signatures or rules. An adversarial mechanism is added to the DQL-based training procedure. A DQN agent is given training for recognizing intrusions by optimizing the forecasted reward function. Also, another DQN agent is supplemented for generating adversarial information throughout the training procedure by generating perturbations in the attack and regular data. Motwakel et al. [21] propose an efficient Enhanced Crow Search Algorithm with DL-Driven Cyber-attack Detection (ECSADL-CAD) methodology for the Software-Defined Network (SDN)-based IoT atmosphere. This proposed technique first performs pre-processing. Later, the Reinforced DBN (RDBN) approach is implemented for attack recognition. Finally, the hyperparameter tuning procedure of the proposed model is achieved by using the ECSA-based model.

3. Methodology

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

In this study, we focus on the design and development of the pNHSS-CAD technique to improve network security. To accomplish that, the pNHSS-CAD technique comprises a selection of features using WOA, pNHSS-based detection, and parameter optimization using FF. Fig. 1 depicts the workflow of the pNHSS-CAD technique.

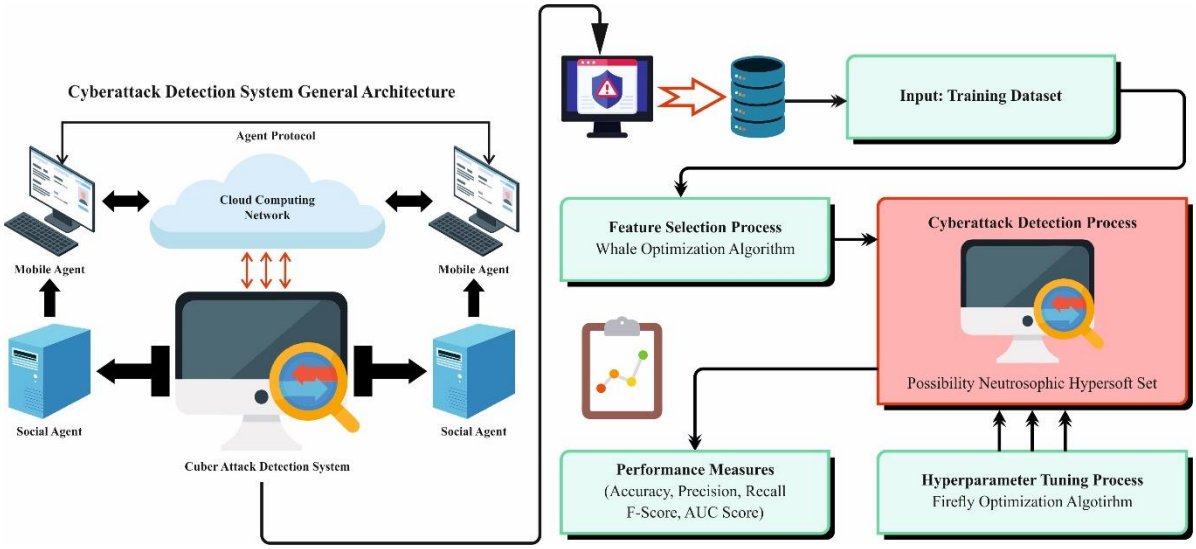

Figure 1: Workflow of pNHSS-CAD technique

A. Modeling of WOA for Dimensionality Reduction

Primarily, the pNHSS-CAD method has its formation in feature selection with the WOA. WOA is nothing but an optimizer model, which is stimulated by humpback whales [22]. When they determine their objective, humpback whales can enclose it. The WOA technique functions below the principle that the existing finest candidate solution is the target of notice. After the finest searching agent is nominated, the residual searching agents will try to appeal nearer to it.

The behavior of whales was established over Eqs. (1)-(2):

$$D = |C \cdot X^*(t) - X(t)| \tag{1}$$

$$X(t+1) = X^*(t) - A.D \tag{2}$$

Whereas t signifies the present iteration, X^* embodies the position vector of the finest result, A, and C refers to the vector of coefficient, || signifies the absolute value, X indicates the location vector, and (.) denotes element-wise multiplication. After every cycle, X^* must be altered. A and C vectors are intended to be utilized.

EXPLOITATION STAGE

Dual tactics were formed to exactly pretend the humpback behavior of whales in bubble nets:

1) SHRINKING ENCIRCLING MECHANISM

The mechanism of shrinking encircling is parallel to GWO.

2) SPIRAL UPGRADING LOCATION

The initial stage is to define the space among the whale at the location (X, Y) and the target at the location(X^*, Y^*). A spiral calculation (Eq. (3)) is constructed among the whale location and its victim to emulate the spiral movement.

$$X(t+1) = D' \cdot exp^{bl} \cdot cos(2\pi l) + X^*(t) \tag{3}$$

Here, D' is signified in Eq. (4) and designates the space amongst the ith whale, b denotes a constant to define the logarithmic spiral shape, l represents the randomly generated values in [1 and 1] and (.) symbol refers to an element-wise multiplication.

$$D' = |X^*(t) - X(t)| \tag{4}$$

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

The humpback whales swim at the same time in a falling circle and helix shape near their victim. To describe this parallel behavior, we accept a 50% possibility of selecting both the shrinking encirclement device and the helix method to upgrade. Furthermore, according to the bubble-net model, humpback whales hunt for target randomly. The expression is given below.

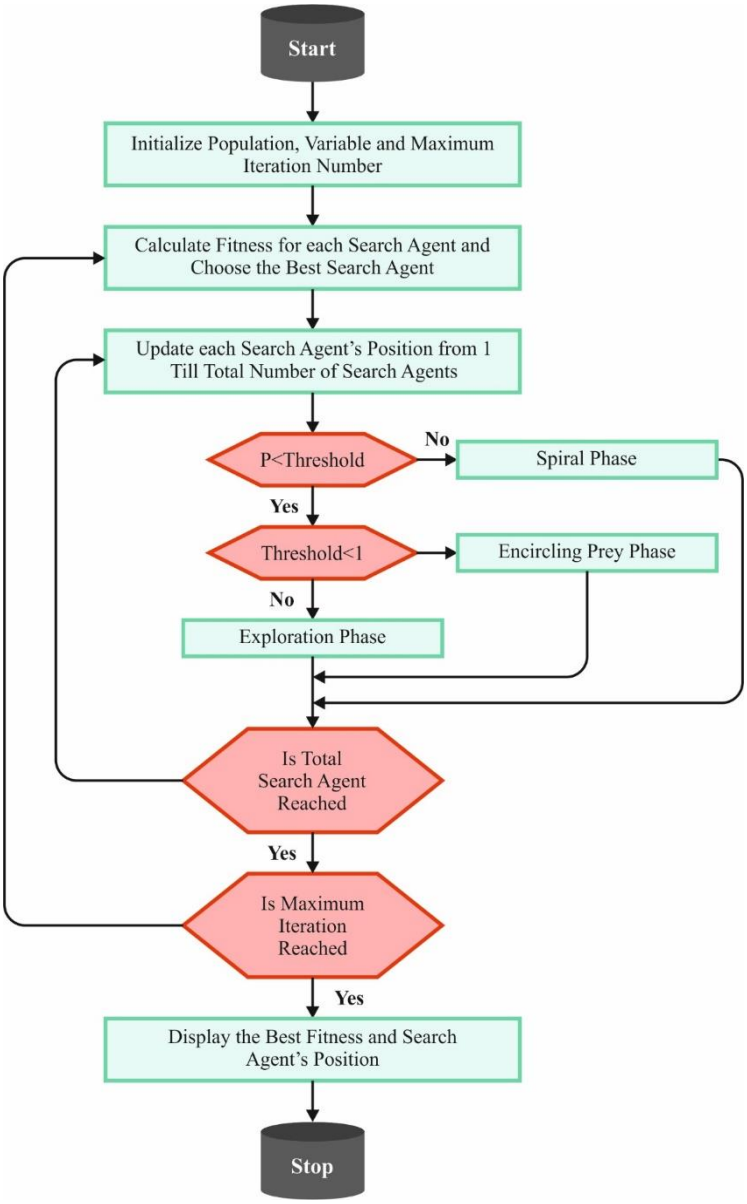

Figure 2: Flowchart of WOA

EXPLORATION STAGE

Prey exploration can be completed utilizing a similar method dependent upon an alteration to the A vector. So, to strengthen the searching agent to travel away from a position whale, A with arbitrary values bigger or lesser than l was used. The searching agent location is upgraded depending upon an arbitrarily selected searching agent at the time of the exploration stage as divergent to the finest searching agent so far learned during the stage of exploitation. With aid of this technique, $|A| > 1$ is a highlight exploration, so the WOA model is capable of a global search. This stage is expressed mathematically as below:

$$D = |C \cdot X_{rand}(t) - X(t)| \quad (5)$$

$$X(t+1) = X_{rand}(t) - A \cdot D \quad (6)$$

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

Here, X_{rand} represents the randomly generated location vector selected from the existing population. Fig. 2 illustrates the flowchart of WOA.

The fitness function (FF) utilized in the WOA is proposed to contain a stability among the integer of designated features in each solution (minimum) and the classifier accuracy (maximum) gained by employing these nominated features, Eq. (7) denotes the FF to assess solution.

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \tag{7}$$

Whereas, $\gamma_R(D)$ signifies the classifier rate of error of an assumed classifier. $|R|$ is the cardinality of the nominated sub-set and $|C|$ is the complete integer of features, α and β are dual parameters, which is equivalent to the position of classifier excellence and sub-set length. $\in [1,0]$ and $\beta = 1 - \alpha$.

B. Classifier Selection using pNHSS

Next, the pNHs-set classifier is employed for the robust detection and identification of cyber-attacks. This section provides a few basic terms and descriptions by studying the current works [23]:

Description 1. *An* Hs-set over $\mathcal{Z}$ denotes set of pairs $(\mathcal{W}, \mathcal{H})$, whereas $\mathcal{H}$ denotes the Cartesian product of $\mathcal{H}^i, i = 1,2,3, \dots, n, \mathcal{H}^i \cap \mathcal{H}^j = \emptyset$ for every $i \neq j$ containing attributes values $\hat{a}, i = 1,2,3, \dots, n, a^i \neq \hat{a}^j, i \neq j$, correspondingly. Every $\mathcal{W}(\hat{h}_\alpha), \alpha = 1,2,3, \dots, k$ represents the sub-sets of $\mathcal{Z}$ and is recognized as multi-argument estimated element of Hs-set $(\mathcal{W}, \mathcal{H})$. Also, *an* Hs-set $(\mathcal{W}, \mathcal{H})$ is seen as a parameterized range of the preliminary universe $\mathcal{Z}$.

Description 2. An Hs-set $(\mathcal{W}, \mathcal{H})$ is named a fuzzy Hs-set. If $\mathbb{P}(\mathcal{Z})$ in $\mathcal{W}$:$\mathcal{H} \to \mathbb{P}(\mathcal{Z})$ is substituted with $F(\mathcal{Z}), IF(\mathcal{Z})$ and $\mathbb{N}(\mathcal{Z})$, whereas $F(\mathcal{Z}), IF(\mathcal{Z})$ and $\mathbb{N}(\mathcal{Z})$ are relations of fuzzy, intuitionistic fuzzy, and neutrosophic sub-sets on $\mathcal{Z}$, correspondingly.

Description 3. A pNs-set $\mathfrak{R}_\mathcal{S}$ is definite below

$\mathfrak{R}_\mathcal{S} = \{(\zeta_\mathcal{S}(\hat{a}), \psi_\mathcal{S}(\hat{a})), \zeta_\mathcal{S}(\hat{a}) \in \mathbb{N}(\mathcal{Z}), \psi_\mathcal{S}(a) \in \mathbb{F}(\mathcal{Z})$ and $\hat{a} \in \mathbb{A}\}$ where $\mathbb{A} \subseteq \mathbb{E}$ (a parameter set), $\zeta_\mathcal{S} : \mathbb{A} \to \mathbb{N}(\mathcal{Z})$, and $\psi_\mathcal{S}$:$\mathbb{A} \to \mathbb{F}(\mathcal{Z})$.

This part provides the description and set-theoretic processes of the $pNHs$-set with mathematical instances. It is a substance of general opinion that in any employment procedure, a jury is created to interview the analyzed applicants first. This jury generally contains a leader and other members, who know the specific domain. Every group of followers of the jury is focused on measuring the ability and fitness of the applicants. Many engaged to deliver their professional thoughts in 3-D, that is., recommend, discard, or be neutral about the valuation of candidate's equivalent to multi-argument groups. The leader is authorized to examine the professional views with their stage of approval. In brief, 3 states in this situation should be faced in a single method:

1. The condition states the vital identification into their correlated sub-parametric value in the procedure of dissimilar sets.
2. The condition needs the assertion of the maa-function, which is capable of under-taking the multi-argument area.
3. The condition that requires the decision-makers to offer their skilled decisions in the procedure of neutrosophic value that assurance the 3D.
4. The condition needs the reflection of the prospect grade to assess the acceptance level of the professional decisions.

The existing works are insufficient to deliver any numerical method to challenge every abovementioned condition together in a single method. This fault remains the inspiration of this research. The developed method pNHs-set, is proficient in handling all the above-mentioned conditions together as one framework. The pNHs-set contains 3 portions such as hypersoft set, neutrosophic set, and possibility-degree-based set. The $pNHs$-set achieves conditions of 1 and 2 by using a hypersoft set; condition 3 is attempted by employing the neutrosophic set; the final condition 4 is handled by employing the possibility-degree-based set. Numerous other states of reality are accessible like medical analysis, project selection, product selection, and analysis of risk, and many need the setting of pNHs.

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

Description 4. A $pNHs$-set $\mathfrak{F}\psi$ over hypersot universe (Z, J) is specified by the sets $\psi = \{\left(\delta, \left\{\left(\frac{\hat{z}}{F(\delta)(\hat{z})}, \psi(\delta)(Z)\right) : Z \in \mathcal{Z}\right\}\right) : \delta \in \mathcal{J}\}$ whereas $\mathcal{J}_i$ denotes the non-overlapping parametric parameter sets a_i, $i = 1,2, \ldots, n$, correspondingly, like $\mathcal{J} = \mathcal{J}_1 \times \mathcal{J}_2 \times \cdots \times \mathcal{J}_n, F_\psi : \mathcal{J} \to \mathbb{N}_Z \times I_Z, \mathfrak{F}: J \to \mathbb{N}_Z, \psi: J \to I_Z, I_Z \in \mathbb{F}(\mathcal{Z})$, and $\mathbb{N}_Z \in \mathbb{N}(\mathcal{Z})$, correspondingly; $\mathfrak{F}(\delta)(\hat{z})$ represents the neutrosophic integer of $\hat{z} \in \mathcal{Z}$ in $F(\delta)$, and $\psi(\delta)(\hat{z})$ refers to the possible degree of $\hat{z} \in \mathcal{Z}$ in $F(\delta)$. So, $F_\psi(\delta_i)$ is definite below:

$$\mathfrak{F}_\psi(\delta_i) = \left\{\left(\frac{\hat{z}}{\mathfrak{F}(\delta_i)(\hat{z}_1)}, \psi(\delta_i)(\hat{z}_1)\right), \left(\frac{\hat{z}}{\mathfrak{F}(\delta_i)(\hat{z}_2)}, \psi(\delta_i)(\hat{z}_2)\right), \ldots, \left(\frac{\hat{z}}{\mathfrak{F}(\delta_i)(\hat{z}_n)}, \psi(\delta_i)(\hat{z}_n)\right)\right\}$$

It is notable that, for accessibility, the $pNHs$-set is signified by F_ψ and Ω_{pnhss} denotes its family.

Instance 1. Assume the health supervisor of a municipal hospital generates a team containing heart experts to measure the heart illnesses by detecting suitable parameters. The 4 kinds of heart illnesses are taken into attention, which are surrounded in discourse set $\mathcal{Z} = \{\widehat{D}_1, \widehat{D}_2, \widehat{D}_3, \widehat{D}_4\}$. The members of the group have a parameter set $a_1 = chest$ pain type, a_2 =resting blood pressure (mmHg), and $a_3 = serum$ cholesterol (mg/dL) with their common consensus. After the clear surveillance, the parameters are categorized into their associated parametric-valued sets are $J_1 = \{a_{11}$ =typicalangina,$a_{12} = atypicalangina\}$, $J_2 = \{a_{21} = 150, a_{22} = 180\}$, and $J_3 = \{a_{31} = 320\}$, correspondingly. To get the tuples of parametric, their Cartesian product is calculated as $\mathcal{J} = \mathcal{J}_1 \times \mathcal{J}_2 \times \mathcal{J}_3 = \{\delta_1, \delta_2, \delta_3, \delta_4\}$. By the presence of parametric tuples, the associates are focused to deliver their thoughts in the method of neutrosophic elements. The received thoughts are together as multi-argument estimated basics of $pNHs$-set that assumed as follows:

$$\mathfrak{F}_\psi(\delta_1) = \left\{\left(\frac{\widehat{D}_1}{<0.3,0.1,0.2>}, 0.2\right), \left(\frac{\widehat{D}_2}{<0.4,0.2,0.3>}, 0.3\right), \left(\frac{\widehat{D}_3}{<0.5,0.3,0.4>}, 0.4\right), \left(\frac{\widehat{D}_4}{<0.6,0.4,0.5>}, 0.5\right)\right\}$$

$$F_\psi(\delta_2) = \left\{\left(\frac{\widehat{D}_1}{<0.7,0.2,0.3>}, 0.8\right), \left(\frac{\widehat{D}_2}{<0.6,0.3,0.4>}, 0.8\right), \left(\frac{\widehat{D}_3}{<0.6,0.4,0.5>}, 0.7\right), \left(\frac{\widehat{D}_4}{<0.5,0.5,0.6>}, 0.6\right)\right\}$$

$$F_\psi(\delta_3) = \left\{\left(\frac{\widehat{D}_1}{<0.5,0.1,0.1>}, 0.1\right), \left(\frac{\widehat{D}_2}{<0.4,0.1,0.2>}, 0.2\right), \left(\frac{\widehat{D}_3}{<0.5,0.1,0.3>}, 0.3\right), \left(\frac{\widehat{D}_4}{<0.6,0.2,0.4>}, 0.4\right)\right\}$$

$$F_\psi(\delta_4) = \left\{\left(\frac{\widehat{D}_1}{<0.7,0.1,0.2>}, 0.2\right), \left(\frac{\widehat{D}_2}{<0.5,0.1,0.3>}, 0.3\right), \left(\frac{\widehat{D}_3}{<0.6,0.4,0.4>}, 0.4\right), \left(\frac{\widehat{D}_4}{<0.7,0.2,0.5>}, 0.5\right)\right\}$$

Then, $\mathfrak{F}_\psi$ denotes a $pNHs$-set over $(, J)$. Its representation of matrix is:

$$F_\psi = \begin{pmatrix} (\prec 0.3,0.1,0.2 \succ, 0.2) & (\prec 0.4,0.2,0.3 \succ, 0.3) & (\prec 0.5,0.3,0.4 \succ, 0.4) & (\prec 0.6,0.4,0.5 \succ, 0.5) \\ (\prec 0.7,0.2,0.3 \succ, 0.8) & (\prec 0.6,0.3,0.4 \succ, 0.8) & (\prec 0.6,0.4,0.5 \succ, 0.7) & (\prec 0.5,0.5,0.6 \succ, 0.6) \\ (\prec 0.5,0.1,0.1 \succ, 0.1) & (\prec 0.4,0.1,0.2 \succ, 0.2) & (\prec 0.5,0.1,0.3 \succ, 0.3) & (\prec 0.6,0.2,0.4 \succ, 0.4) \\ (\prec 0.7,0.1,0.2 \succ ,0.2) & (\prec 0.5,0.1,0.3 \succ ,0.3) & (\prec 0.6,0.4,0.4 \succ ,0.4) & (\prec 0.7,0.2,0.5 \succ ,0.5) \end{pmatrix}.$$

In this $pNHs$-set, the 1st component $(\prec 0.3,0.1,0.2 \succ ,0.2)$ indicates that every decision-maker has delivered together the membership grade as 0.3 (30%), indeterminate grade as the 0.1(10%), and non-membership grade as the 0.2 (20%) for illness D_1, and a possibility degree of 0.2 (20%) is allocated by the leader for the approval of professional thoughts $\prec 0.3,0.1,0.2 \succ toD_1$ by restraining in opinion δ_1. Likewise, other estimated origins and their values were calculated in a similar method

Description 5. Assume that $\mathfrak{A}_\psi, \mathfrak{B}_\zeta \in \Omega_{pnhss/}$ then:

(i) $\mathfrak{A}_\psi \cup \mathfrak{B}_\zeta$ denotes a $pNHs$-set C_ν with $C(\delta) = \sqcup \{\mathfrak{A}(\delta), \mathfrak{B}(\delta)\}$, and $\nu(\delta) = \max\{\psi(\delta), \zeta(\delta)\}$.

(ii) $\mathfrak{A}_\psi \cap \mathfrak{B}_\zeta$ represents the $pNHs$-set $\mathfrak{D}_\omega$ with $\mathfrak{D}(\delta) = \sqcap \{\mathfrak{A}(\delta), \mathfrak{B}(\delta)$, and $\omega(\delta) = \min\{\psi(\delta), \zeta(\delta)\}$. Where, $\sqcup$ and $\sqcap$ represents the union and intersection of neutrosophic, correspondingly.

Instance 2. Assume the data from Instance 1, dual $pNHs$-sets $\mathfrak{A}_\psi, \mathfrak{B}_\zeta \in \Omega_{pnhss}$ are built whose matrix representations are delivered below

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

$$\mathfrak{A}_{\psi} = \begin{pmatrix} (\prec 0.1,0.2,0.3 \succ, 0.2) & (\prec 0.2,0.3,0.4 \succ, 0.3) & (\prec 0.3,0.4,0.5 \succ, 0.4) & (\prec 0.4,0.5,0.6 \succ, 0.5) \\ (\prec 0.5,0.5,0.6 \succ, 0.8) & (\prec 0.6,0.4,0.5 \succ, 0.8) & (\prec 0.7,0.3,0.4 \succ, 0.7) & (\prec 0.9,0.1,0.2 \succ, 0.6) \\ (\prec 0.4,0.3,0.4 \succ, 0.1) & (\prec 0.6,0.4,0.5 \succ, 0.2) & (\prec 0.7,0.2,0.3 \succ, 0.3) & (\prec 0.4,0.1,0.2 \succ, 0.4) \\ (\prec 0.6,0.2,0.3 \succ ,0.2) & (\prec 0.7,0.3,0.4 \succ ,0.3) & (\prec 0.5,0.2,0.3 \succ ,0.4) & (\prec 0.7,0.2,0.3 \succ ,0.5) \end{pmatrix}$$

and

$$\mathfrak{B}_{\zeta} = \begin{pmatrix} (\prec 0.2,0.1,0.2 \succ, 0.3) & (\prec 0.3,0.2,0.3 \succ, 0.4) & (\prec 0.4,0.3,0.4 \succ, 0.5) & (\prec 0.5,0.4,0.5 \succ, 0.6 \\ (\prec 0.6,0.4,0.5 \succ, 0.9) & (\prec 0.7,0.3,0.4 \succ, 0.9) & (\prec 0.8,0.2,0.3 \succ, 0.8) & (\prec 1.0,0.0,0.1 \succ, 0.7) \\ (\prec 0.5,0.2,0.3 \succ, 0.2) & (\prec 0.7,0.3,0.4 \succ, 0.3) & (\prec 0.8,0.1,0.2 \succ, 0.4) & (\prec 0.5,0.0,0.1 \succ, 0.5) \\ (\prec 0.7,0.1,0.2 \succ ,0.3) & (\prec 0.8,0.2,0.3 \succ ,0.4) & (\prec 0.6,0.1,0.2 \succ ,0.5) & (\prec 0.8,0.1,0.2 \succ ,0.6) \end{pmatrix}$$

Then $C_{\nu} = \mathfrak{A}_{\psi} \cup \mathfrak{B}_{\zeta} = \mathfrak{B}_{\zeta}$ and $\mathfrak{D}_{\omega} = \mathfrak{A}_{\psi} \cap \mathfrak{B}_{\zeta} = \mathfrak{A}_{\psi}$.

C. pNHSS Model Optimization

Finally, the FF technique is applied for hyperparameter selection. In recent years, nature has been a major stimulation in making a wide range of innovative techniques [24]. The important advantage of developing methods that need particular features to be improved is the outcome of real-time problems. Transnational approaches for the optimizer process have been frequently utilized. Firefly has a method stimulated by fireflies' reproducing or flashing activities. By comparison with standard techniques such as PSO, ABC, and ACO. These methods are more available, implementable, and comprehensible. Fireflies can be lightning bugs that release light sources for attracting prey or partners employing a unique frequency. The radius (R) and luminosity (I) of the light radiated through the pests are adversely proportionated. Any standards utilize when applying the firefly algorithm (FA).

- Fireflies, unrelated to gender, can attract one another.
- Attraction must be directly connected to luminosity and inversely equal to their distance.
- The foremost function is to extent the quantity of light the firefly produces.

The working principle describing the method's efficiency is given below.

The simplest equation of luminous flux $f(r)$ varies reliant upon the opposite square law.

$$F(r) = \frac{f_s}{r^2}. \tag{8}$$

Now, $f(r)$ denotes the luminous flux, r denotes the distance between the source and the object, and fs represents the source of the object.

Attractiveness and light intensity

A neighboring firefly could be identified by the luminous intensity and desirability of a close firefly, and the attraction of the firefly could be described as $\propto$:

$$\infty = \infty_0 e^{-r^2} \tag{9}$$

To find the firefly distance at the source $r = 0$.

Distance

A basic mathematical formula can estimate the distance among the dual adjacent fireflies:

$$Q_{ij} = \|d_i - d_j\| \tag{10}$$

Now, the variables i and j refer to the drive of the firefly in the ith place to the jth position.

The firefly model derives an FF to achieve enhanced classifier solution. It defines a positive numeral to signify the improved solutions of the candidate. In this research work, the minimizer of the classifier rate of error is measured as the FF, as specified in Eq. (11).

$$fitness(x_i) = ClassifierErrorRate(x_i)$$

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

$$= \frac{No.of\ misclassified\ instances}{Total\ no.of\ instances} * 100 \quad (11)$$

4. Experimental Validation

The experimental evaluation of pNHSS-CAD technique is verified utilizing a benchmark dataset. It contains 148517 instances with 5 class labels as represented in Table 1.

Table 1: Details of Dataset

Classes	No. of Instances
Normal	77054
DoS	53385
Probe	14410
R2L	3416
U2R	252
Total Instances	148517

In Table 2, the overall attack detection results of the pNHSS-CAD method are highlighted. The results stated that the pNHSS-CAD approach has the effectual capability of identifying attacks.

In Fig. 3, the average results of the pNHSS-CAD technique obtained to detect intrusions under 80 %TRAS is illustrated. The figure represented that the pNHSS-CAD technique effectively recognizes the attacks. It is observable that the pNHSS-CAD technique reaches average $accu_y$ of 99.39%, $prec_n$ of 90.58%, $reca_l$ of 93.26%, F_{score} of 91.85%, and AUC_{score} of 96.41%.

In Fig. 4, the average outcomes of the pNHSS-CAD system attained to identify intrusions under 20%TESS is demonstrated. The figure signified that the pNHSS-CAD system efficiently identifies the attacks. It is noticeable that the pNHSS-CAD method attains an average $accu_y$ of 99.36%, $prec_n$ of 90.04%, $reca_l$ of 91.01%, F_{score} of 90.51%, and AUC_{score} of 95.27%.

Table 2 Attack detection results of pNHSS-CAD technique under 80:20 of TRAS/TESS

Classes	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	AUC_{score}
TRAS (80%)					
Normal	99.26	99.43	99.15	99.29	99.27
DoS	98.87	98.39	98.46	98.42	98.78
Probe	99.21	96.18	95.66	95.92	97.63
R2L	99.72	91.14	97.25	94.10	98.51
U2R	99.90	67.74	75.77	71.53	87.86
Average	99.39	90.58	93.26	91.85	96.41
TESS (20%)					
Normal	99.23	99.51	99.02	99.26	99.24
DoS	98.81	98.09	98.61	98.35	98.77
Probe	99.19	96.13	95.39	95.76	97.49
R2L	99.70	90.95	96.51	93.64	98.14
U2R	99.87	65.52	65.52	65.52	82.72
Average	99.36	90.04	91.01	90.51	95.27

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

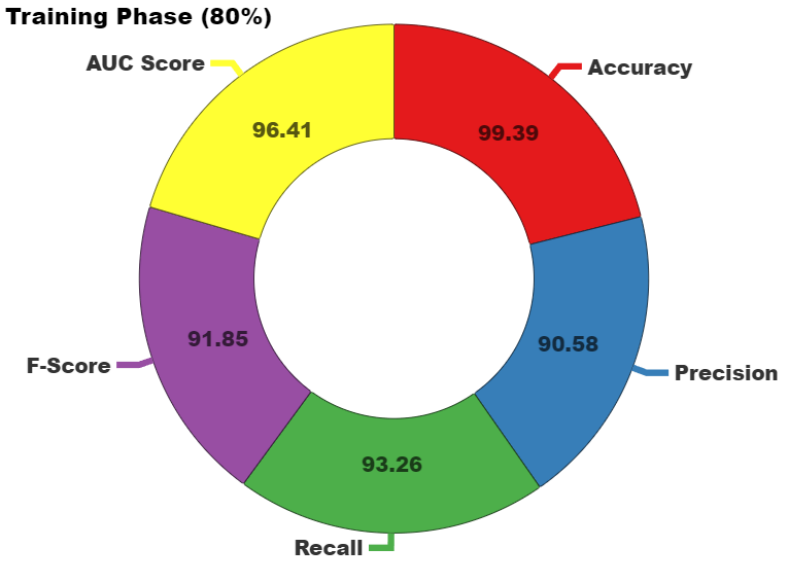

Figure 3: Average outcome of pNHSS-CAD technique under 80% TRAS

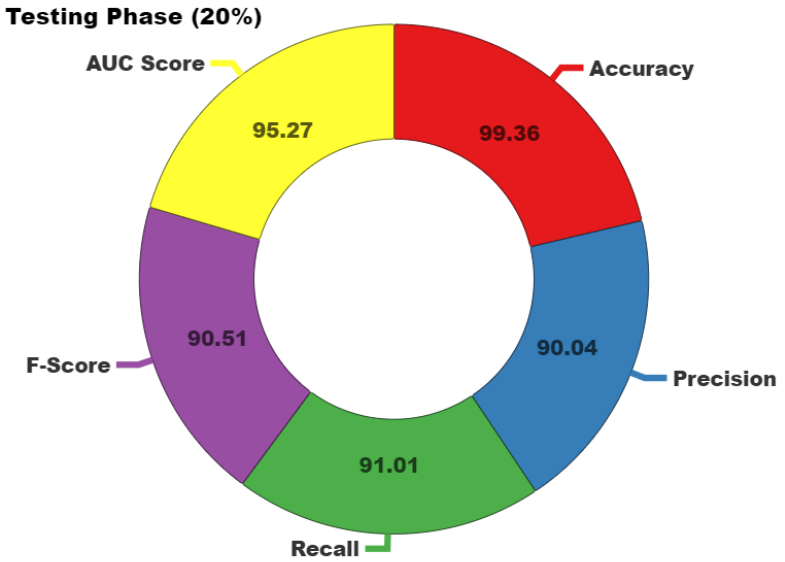

Figure 4: Average outcome of pNHSS-CAD technique under 20% TESS

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

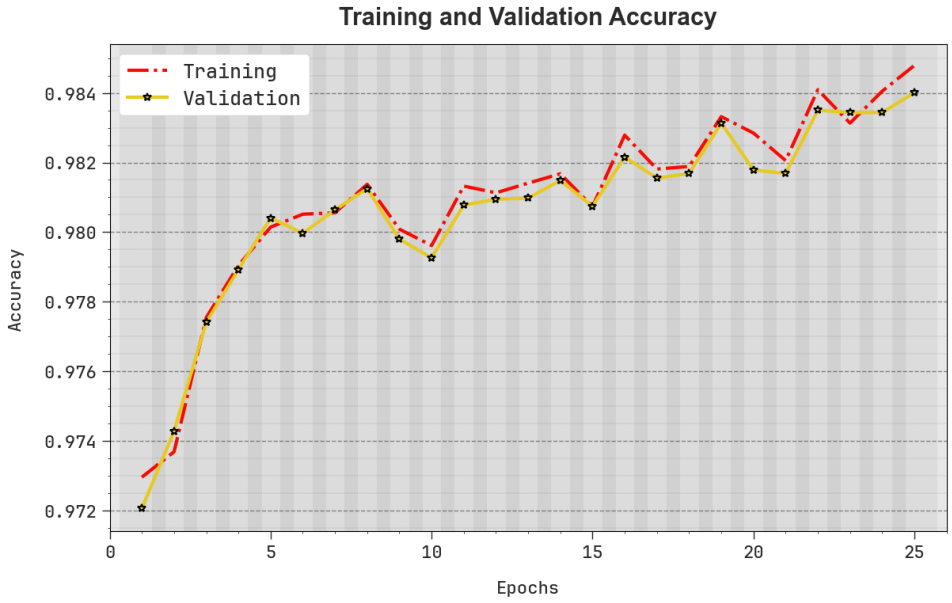

Figure 5: $Accu_y$ curve of pNHSS-CAD technique

In Fig. 5, the training and validation accuracy outcomes of the pNHSS-CAD method are established. The accuracy values are calculated throughout 0-25 epochs. The figure emphasized that the training and validation accuracy values display a rising tendency which reported the capability of the pNHSS-CAD system with enhanced performance over many iterations. Moreover, the training and validation accuracy remains nearer over the epochs, which specifies less minimal overfitting and shows improved performance of pNHSS-CAD method, guaranteeing consistent prediction on hidden samples.

In Fig. 6, the training and validation loss graph of the pNHSS-CAD technique is shown. The loss values are computed throughout 0-25 epochs. It is denoted that the training and validation accuracy values demonstrate a declining tendency, alerting the skill that notified the skill of the pNHSS-CAD technique in balancing a trade-off between data fitting and generalization. The continual decrease in loss values also guarantees the greater performance of the pNHSS-CAD approach and tunes the prediction outcomes over time.

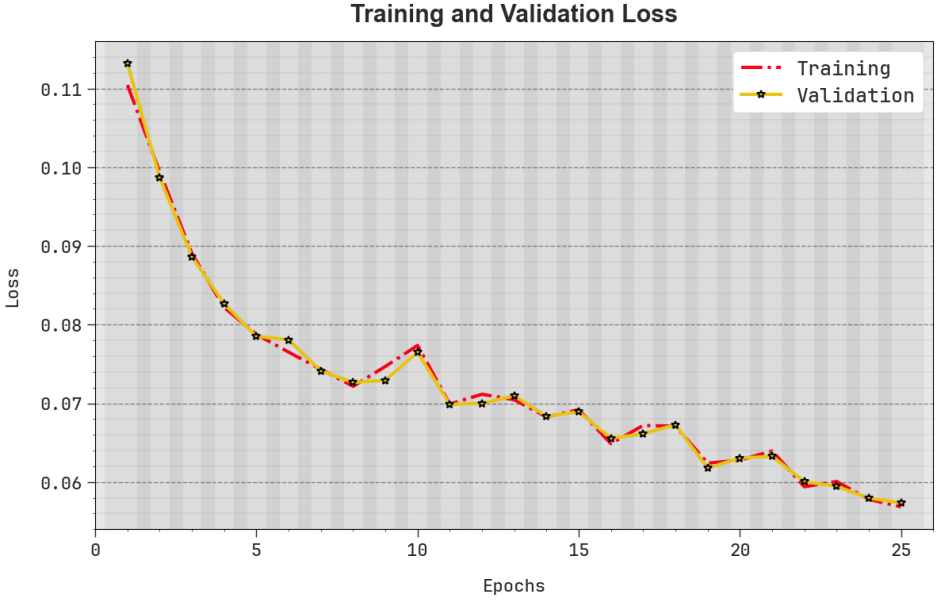

Figure 6: Loss curve of pNHSS-CAD technique

In Fig. 7, the precision-recall (PR) curve analysis of the pNHSS-CAD system provides an interpretation of its performance by plotting Precision against Recall for every class. The figure displays that the pNHSS-CAD method

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

constantly achieves enhanced PR values across dissimilar class labels, demonstrating its capability to preserve a major part of true positive predictions between every positive prediction (precision) while also capturing a huge proportion of actual positives (recall). The sturdy rise in PR results between all classes represents the efficacy of the pNHSS-CAD technique in the classification procedure.

In Fig. 8, the ROC curve of the pNHSS-CAD system is studied. The outcomes suggest that the pNHSS-CAD technique achieves improved ROC outcomes over every class, signifying a major ability to discriminate the classes. This reliable trend of upgraded ROC values over many classes indicates the proficient performance of pNHSS-CAD technique in predicting classes, emphasizing the robust nature under the classification method.

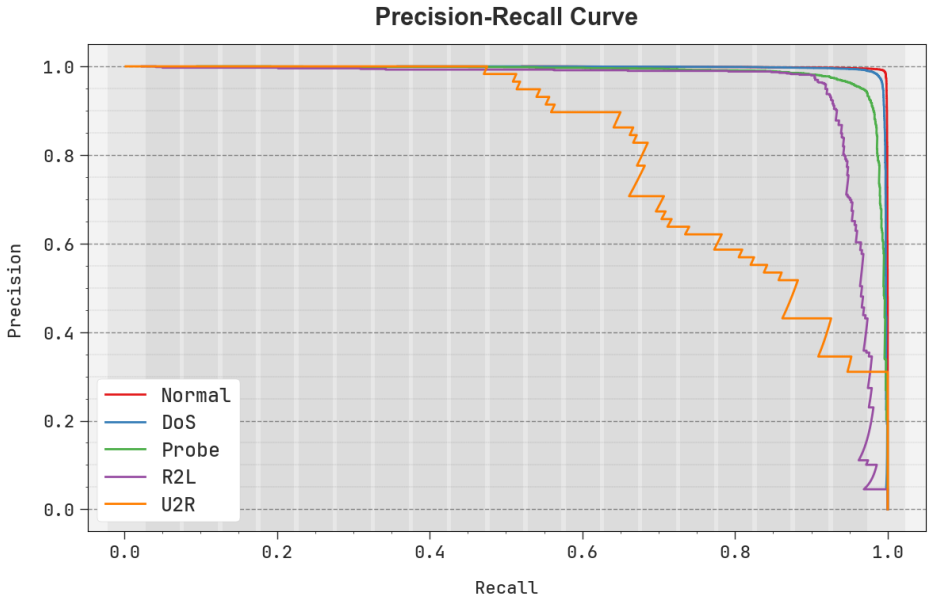

Figure 7: PR curve of pNHSS-CAD technique

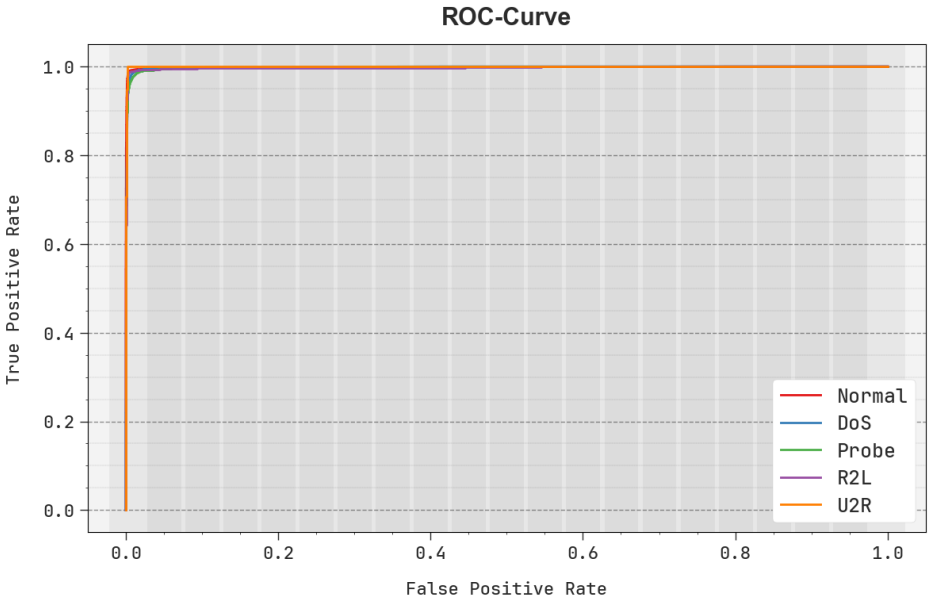

Figure 8: ROC curve of pNHSS-CAD technique

In Table 3 , the overall results of the pNHSS-CAD technique are compared with recent models [19]. The results reported that the NSL-KDD IoT, AE-MLID, and DL-NIDS models have shown poor performance over other models. In line with this, the DL-Improved ID, ADNT-ELM, and DL-DCSCA IoT CN methods have accomplished closer performance. Meanwhile, the HBA-OHDBN model has managed to report reasonable results. Nevertheless, the pNHSS-CAD system demonstrates superior performance with maximum $accu_y$ of 99.36%, $prec_n$ of 90.04%,

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

$reca_l$ of 91.01%, and F_{score} of 90.51%. Therefore, the pNHSS-CAD technique has the ability to detect attacks in the IoT platform.

Table 3: Comparative analysis of pNHSS-CAD technique with recent methods

Models	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
AE-MLID	85.20	73.46	72.34	71.39
NSL-KDD IoT	78.50	71.94	70.86	71.04
DL-Improved ID	94.60	70.91	69.17	74.27
DL-NIDS	88.40	71.01	70.28	70.31
ADNT-ELM	91.70	73.30	70.82	73.95
DL-DCSCA IoT CN	98.20	72.01	72.77	73.20
HBA-OHDBN	99.21	76.26	75.04	75.63
pNHSS-CAD	99.36	90.04	91.01	90.51

5. Conclusion

In this study, we focus on the design and development of pNHSS-CAD technique to improve network security. To accomplish that, the pNHSS-CAD technique comprises a selection of features using WOA, pNHSS-based detection, and parameter optimization using FF. The pNHSS-CAD method has its formation in feature selection with the WOA, which successfully recognizes the important features from the data, thus improving processing speed and reducing dimensionality. Following feature selection, the pNHs-set classifier is employed for the robust detection and identification of cyber-attacks, which leverages the power of neutrosophic set to deal with ambiguity and uncertainty in the information. The FF technique is applied for hyperparameter fine-tuning, which ensures the model operates at maximum effectiveness to enhance the performance of the classification. This wide-ranging method leads to a very efficient cyberattack recognition method, which can able to accurately mitigate and identify risks in the real world.

Funding: "This research received no external funding"

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

References

[1] Smarandache, F., Neutrosophic set a generalization of the intuitionistic fuzzy sets. Inter. J. Pure Appl. Math., 24, 287 – 297, 2005.
[2] Das, S.K. and Edalatpanah, S.A., 2020. A new ranking function of triangular neutrosophic number and its application in integer programming. International Journal of Neutrosophic Science, 4(2), pp.82-92.
[3] Dhar, M., 2020. Neutrosophic soft block matrices and some of its properties. Int J Neutrosophic Sci, 12(1), pp.39-49.
[4] Chinnadurai, V. and Sindhu, M.P., 2020. An introduction to neutro-fine topology with separation axioms and decision making. International Journal of Neutrosophic Science (IJNS) Volume 12, 2020, p.11.
[5] Chinnadurai, V. and Sindhu, M.P., 2020. An introduction to neutro-fine topology with separation axioms and decision making. International Journal of Neutrosophic Science (IJNS) Volume 12, 2020, p.11.
[6] Edalatpanah, S.A., 2020. A direct model for triangular neutrosophic linear programming. International journal of neutrosophic science, 1(1), pp.19-28.
[7] Das, S.; Manchala, Y.; Rout, S.K.; Kumar Panda, S. Deep Learning and Metaheuristics based Cyber Threat Detection in Internet of Things Enabled Smart City Environment. Res. Sq. 2023. preprint.
[8] Asiri, M.M.; Mohamed, H.G.; Nour, M.K.; Al Duhayyim, M.; Aziz, A.S.A.; Motwakel, A.; Zamani, A.S.; Eldesouki, M.I. Hybrid Metaheuristics Feature Selection with Stacked Deep Learning-Enabled Cyber-Attack Detection Model. Comput. Syst. Sci. Eng. 2023, 45, 1679–1694.
[9] Alohali, M.A.; Elsadig, M.; Al-Wesabi, F.N.; Al Duhayyim, M.; Hilal, A.M.; Motwakel, A. Blockchain Assisted Op-timal Machine Learning Based Cyberattack Detection and Classification Scheme. Comput. Syst. Sci. Eng. 2023, 46, 3583–3598.

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024

[10] Huma, Z.E.; Latif, S.; Ahmad, J.; Idrees, Z.; Ibrar, A.; Zou, Z.; Alqahtani, F.; Baothman, F. A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. IEEE Access 2021, 9, 55595–55605.
[11] Alkatheiri, M.S.; Alghamdi, A.S. Blockchain-Assisted Cybersecurity for the Internet of Medical Things in the Healthcare Industry. Electronics 2023, 12, 1801.
[12] Alajlan, N.N. and Ibrahim, D.M., 2022. TinyML: Enabling of inference deep learning models on ultra-low-power IoT edge devices for AI applications. Micromachines, 13(6), p.851.
[13] Dornadula, V.N. and Geetha, S., 2019. Credit card fraud detection using machine learning algorithms. Procedia computer science, 165, pp.631-641.
[14] Alsaheel, A., Alhassoun, R., Alrashed, R., Almatrafi, N., Almallouhi, N. and Albahli, S., 2023. Deep Fakes in Healthcare: How Deep Learning Can Help to Detect Forgeries. Computers, Materials & Continua, 76(2).
[15] Albahli, S. and Nawaz, M., 2023. MedNet: Medical deepfakes detection using an improved deep learning approach. Multimedia Tools and Applications, pp.1-19.
[16] Aladhadh, S., Alwabli, H., Moulahi, T. and Al Asqah, M., 2022. Bchainguard: a new framework for cyberthreats detection in blockchain using machine learning. Applied Sciences, 12(23), p.12026.
[17] Vaiyapuri, T., Shankar, K., Rajendran, S., Kumar, S., Gaur, V., Gupta, D. and Alharbi, M., 2024. Automated cyberattack detection using optimal ensemble deep learning model. Transactions on Emerging Telecommunications Technologies, 35(4), p.e4899.
[18] Ding, W., Abdel-Basset, M. and Mohamed, R., 2023. DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks. Information Sciences, 634, pp.157-171.
[19] Rao, D.S. and Emerson, A.J., 2024. Cyberattack defense mechanism using deep learning techniques in software-defined networks. International Journal of Information Security, 23(2), pp.1279-1291.
[20] Assiri, F.Y. and Ragab, M., 2023. Optimal deep-learning-based cyberattack detection in a blockchain-assisted IoT environment. Mathematics, 11(19), p.4080.
[21] Hussain, M.M., Khalid, N., Amjad, A. and Shoaib, M., 2024, February. Cyber Attack Identification System Using Deep Learning. In 2024 5th International Conference on Advancements in Computational Sciences (ICACS) (pp. 1-13). IEEE.
[22] Motwakel, A., Alrowais, F., Tarmissi, K., Marzouk, R., Mohamed, A., Zamani, A.S., Yaseen, I. and Eldesouki, M.I., 2023. Enhanced Crow Search with Deep Learning-Based Cyberattack Detection in SDN-IoT Environment. INTELLIGENT AUTOMATION AND SOFT COMPUTING, 36(3), pp.3157-3173.
[23] Saleh, I., Borhan, N., Yunus, A. and Rahiman, W., 2024. Comprehensive Technical Review of Recent Bio-Inspired Population-Based Optimization (BPO) Algorithms for Mobile Robot Path Planning. IEEE Access.
[24] Rahman, A.U., Saeed, M., Mohammed, M.A., Krishnamoorthy, S., Kadry, S. and Eid, F., 2022. An integrated algorithmic MADM approach for heart diseases' diagnosis based on neutrosophic hypersoft set with possibility degree-based setting. Life, 12(5), p.729.
[25] Bacanin, N., Venkatachalam, K., Bezdan, T., Zivkovic, M. and Abouhawwash, M., 2023. A novel firefly algorithm approach for efficient feature selection with COVID-19 dataset. Microprocessors and Microsystems, 98, p.104778.

DOI: https://doi.org/10.54216/IJNS.250103
Received: January 02, 2024 Revised: March 09, 2024 Accepted: June 02, 2024