Interval-Valued Neutrosophic Set with Optimization Algorithm for Cyberthreat Detection and Classification in IoT Infrastructure

Thangam S.[1,*], Jana S.[2]

[1]Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, India

[2]Department of Electronics & Communication Engineering, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai, India

Emails: s_thangam@blr.amrita.edu; drsjana@veltech.edu.in

Abstract

Neutrosophic Logic is an offspring study region in which every intention is projected to hold the proportion of indeterminacy in a subset I, the percentage of truth in a subset T, and the percentage of falsity in subset F. Neutrosophic set (NS) has been effectively used for indeterminate data processing, and establishes benefits to handle with the indeterminacy information of data and is quite a method stimulated for classification application and data analysis. NS delivers an effective and precise method to describe imbalanced data as per the features of the data. Recently, the usage of the Internet of Things (IoT) has enlarged rapidly, and cyber security effects have enlarged beside it. On the state-of-the-art of cyber security is Artificial Intelligence (AI), which employed for the progress of intricate techniques to defense systems and networks, containing IoT systems. Though, cyber-attackers have determined how to develop AI and have started to utilize adversarial AI for accomplishing cybersecurity threats. Therefore, this study designs a new Interval-Valued Neutrosophic Set using Optimization Algorithm-Based Intrusion Detection System (IVNSOA-IDS) technique in IoT cybersecurity. The key objective of the IVNSOA-IDS method rests in the automatic identification of intrusion detection in IoT cybersecurity. In the IVNSOA-IDS technique, data pre-processing is executed to convert the raw data into a compatible format. Besides, the interval-valued neutrosophic set (IVNS) model has been utilized for the automated identification of intrusion detection. Finally, an improved whale optimization algorithm (IWOA) is employed for the better hyperparameter tuning of the IVNS classifier. To demonstrate the enhanced performance of the IVNSOA-IDS technique, an extensive of simulations take place and the performances are inspected under distinct aspects. The experimental outcome reported the advancement of the IVNSOA-IDS methodology under various metrics.

Keywords: Intrusion Detection System; Interval-Valued Neutrosophic Set, Whale Optimization Algorithm; Neutrosophic set; Neutrosophic Logic

1. Introduction

One of the well-organized devices for prediction security in decision making difficulties is the neutrosophic set (NS) and its expansions like interval complex NS (ICNS), interval NS (INS), and complex NS (CNS) [1]. A powerful tool for representing vagueness and ambiguity in decision making is the NS that are more commonly of an intuitionistic fuzzy set (IFS), classical set, and fuzzy set by introducing 3 categories of falsehood, indeterminacy, and truth of a definite statement [2]. They are used in several decision-making methods. However, for adapting NS to more reliable composite cases, INS and CNS are recommended. An Internet of Things (IoT)--based cloud framework is a widespread network, which contains many IoT-supported devices and applications [3]. This infrastructure involves storage and servers, real processing, operation, and basic infrastructures. An IoT-based

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

cloud structure also consists of standards and services vital for managing, securing, and connecting various IoT applications and tools [4]. The growth of the cloud has been seen in the past few decades, and its variations are even increasing in recent decades. IoT takes the initiative among those variants, the IoT. On the other hand, distributed cloud environments, service architectures, management areas, and data center operations are followed in the current trend [5].

The IoT theory has provided the world with a high level of integrity, scalability, accessibility, availability, interoperability, and confidentiality for device networking [6]. Nevertheless, IoTs are prone to cyberattacks owing to the combination of their several attacking surfaces and their novelty and hence sources of uncertainty requirements and standardizations. There is a huge type of cyberattack that attackers can influence against IoTs, based on what aspect of the method they are directing and what they expect to obtain against the attacks [7]. Intrinsically, there is a larger number of investigations into cybersecurity around IoT. These contain Artificial Intelligence (AI) methods for defending IoT models from assailants, generally regarding the diagnosis of peculiar behavior that might direct an attack [8]. Still, regarding IoT, cyber attackers always need control as thereafter need to discover some susceptibility where cybersecurity specialists must protect numerous targets. These have resulted in better usage of AI by cyber attackers also, to thwart the intricate models, which detect anomalous action and pass over unobserved [9]. AI has gained great attention with the development of IoT techniques. Using these developments, AI techniques namely linear regression, support vector machines (SVM), machine learning (ML), decision trees, and neural networks(NN), are employed in IoT cyber-security applications to be capable of recognizing potential attacks and threats [10].

This study designs a new Interval-Valued Neutrosophic Set using Optimization Algorithm-Based Intrusion Detection System (IVNSOA-IDS) technique in IoT cybersecurity. The key objective of the IVNSOA-IDS method rests in the automatic identification of intrusion detection in IoT cybersecurity. In the IVNSOA-IDS technique, data pre-processing is executed to convert the raw data into a compatible format. Besides, the interval valued neutrosophic set (IVNS) model has been utilized for the automated identification of intrusion detection. Finally, an improved whale optimization algorithm (IWOA) is employed for the better parameter tuning of the IVNS method. To demonstrate the enhanced performance of the IVNSOA-IDS technique, a widespread of simulations take place and the outcomes are inspected under distinct measures.

2. Related Works

Amoo et al. [11] propose a widespread analysis of cyber security threats in the age of IoT, classifying them into physical manipulation, malware attacks, data breaches, and furthermore. Countering these threats requires a multidimensional method including effective management practices, device-level security, and network-level measures. Protecting measures are considered, which comprise encryption protocols, secure boot processes, and the execution of IDS. Despite that, insistent challenges, like resource constraints and device diversity, emphasize the need for current development and research. Developing technologies such as edge computing, blockchain, and AI provide encouraging opportunities to boost IoT security. Ahakonye et al. [12] present an article overview from several areas, containing blockchain, AI, Industrial IoT (IIoT), IDS, and IoT to classify developing challenges and tendencies in this domain. A study of different methods integrating blockchain and AI exhibits the capability of incorporating blockchain and AI to modify IDS. This study architecture creates the substructure for additional research and offers a plan for IDS development that is immutable, accessible, decentralized, scalable, and transparent. Nadella and Gonaygunta [13] study the domain of cyber threats, considering phishing, ransomware, denial of service (DoS), and malware attacks. It emphasizes in what way the vital AI is encouraging cybersecurity defense, like IDS, use of intelligent agents, and network security. The paper also addresses the importance of predictive modeling and ML methods in expecting and preventing cyberattacks. Despite the possible assistance of AI-driven cybersecurity, the significance of issues with scalability, data privacy, and human machine assistance cannot be exaggerated.

Adewuyi et al. [14] propose a cybersecurity intersection, data analytics, and IoT, offering an in depth study of the vulnerabilities intrinsic in IoT devices and the advanced security solutions advanced to tackle these problems over datadriven methods. By exploiting innovative data analytics, the author could strengthen the security methods in IoT systems, assuring their flexibility against cyberthreats. In addition, this research finds developing tendencies and upcoming directions for protecting smart environments, proposing useful information on what way the incorporation of these fields could generate a more robust and secure technological substructure for the future. Lai et al. [15] propose extensive research on utilizing ensemble ML techniques for improving IoT cybersecurity through anomaly detection. Instead of utilizing some solitary ML method, ensemble learning integrates the predicting power from various methods, improving their prediction precision in heterogeneous datasets. The author presents an integrated method with ensemble learning, which uses a Bayesian hyperparameter optimizer to adjust

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

to a network atmosphere, which encompasses several readings of IoT sensors. Maghrabi et al. [16] introduce a BESO-HDLBD method in an IoT system. The proposed BESO-HDLBD methodology goal is to solve security problems by recognizing the botnets in the IoT atmosphere. For the recognition of botnet, the BESO-HDLBD system utilizes HDL that is a combination of CNN, attention, and BiLSTM model. The need for the HDL method in botnet recognition uses the sophisticated botnet attacks nature, which recurrently have developing and difficult patterns.

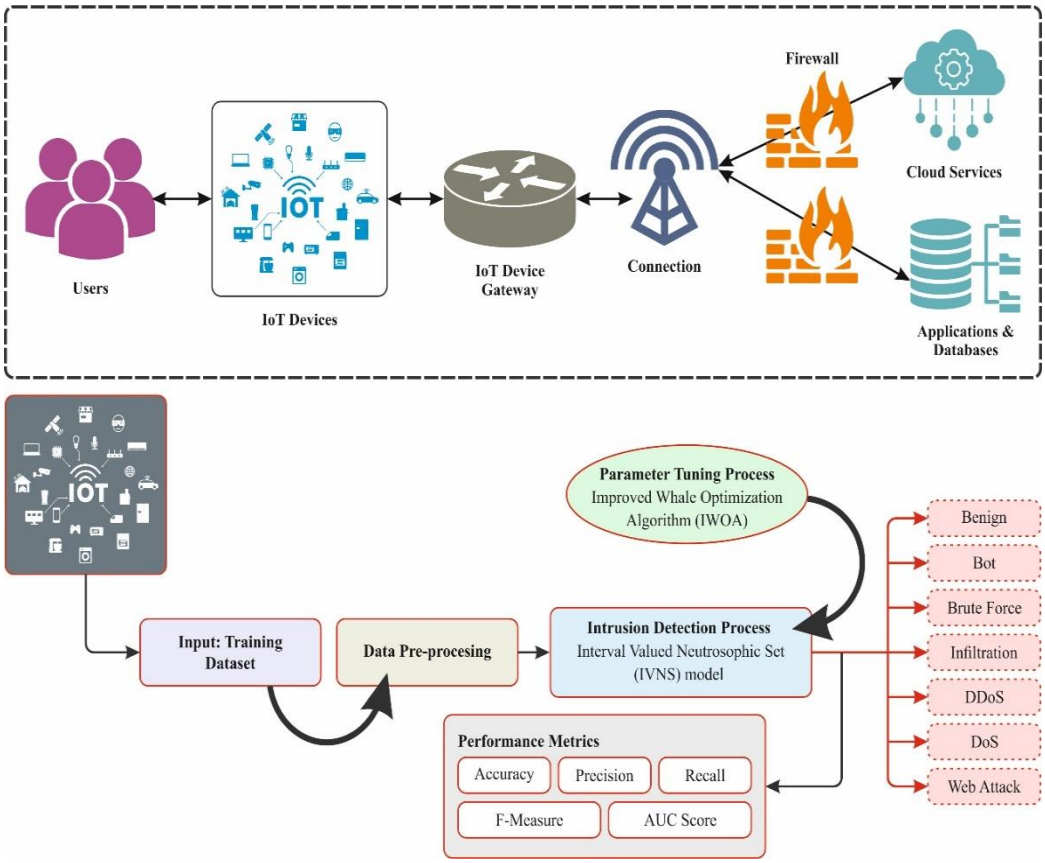

Figure 1. Overall flow of IVNSOA-IDS technique

3. The Proposed Method

In this study, we design a novel IVNSOA-IDS methodology in IoT cybersecurity. The key aim of the IVNSOA-IDS process rests in the automatic identification of intrusion detection in IoT cybersecurity. It contains the three various processes involved in data preprocessing, classification, and hyperparameter tuning. Fig. 1 demonstrates the entire working flow of the IVNSOA-IDS algorithm.

A. Data Preprocessing

Initially, the IVNSOA-IDS process takes place when data pre-processing is executed to convert the raw data into a compatible format. Linear scaling normalization (LSN) is a method employed in IoT cybersecurity to increase IDS. It measures features to an even range, normally [0, 1], making it simpler for ML techniques to perceive anomalies. This normalization decreases the impact of outliers and certifies that every feature donates similarly to the recognition procedure. In the context of IoT, where devices produce various types of data, linear scaling aids in normalizing inputs, foremost for more effective and precise intrusion detection. This technique is vital for preserving the integrity and security of IoT networks.

B. Intrusion Detection using IVNS Classifier

Next, the IVNS model has been utilized for the automated identification of intrusion detection. A short explanation of some basic perceptions of NS, SVNS, IVNS, and some present ranking functions for IVNN are mentioned below [17].

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

Definition2.1: NS is built by $N = \{< x; T_N(x), I_N(x), F_N(x) >, x \in X\}$, whereas X is a universal set of elements x and $T_N(x), I_N(x), F_N(x) : X \rightarrow]^-0, 1^+[$ represents truth, indetermination, and falsity membership function and fulfils the condition,

$$-0 \leq T_N(x) + I_N(x) + F_N(x) \leq 3^+. \quad (1)$$

Definition2.2: SVNS is well-defined by $\dot{N} = \{< x; T_{\dot{N}}(x), I_{\dot{N}}(x), F_{\dot{N}}(x) >, x \in X\}$ and for each

$$x \in X, T_{\dot{N}}(x), I_{\dot{N}}(x), F_{\dot{N}}(x) \in [0,1], \quad (2)$$

$$\dot{N} = \{< \text{x}: \left[T_{\dot{N}}^L(x), T_{\dot{N}}^U(x)\right], \left[I_{\dot{N}}^L(x), I_{\dot{N}}^U(x)\right], \left[F_{\dot{N}}^L(x), F_{\dot{N}}^U(x)\right]$$

$>, x \in X$, where $T_{\dot{N}}(x) = \left[T_{\dot{N}}^L(x), T_{\dot{N}}^U(x)\right] \subseteq [0,1]$,

$$I_{\dot{N}}(x)N = \left[I_{\dot{N}}^L(x), I_{\dot{N}}^U(x)\right] \subseteq [0,1], \quad (3)$$

$F \cdot (x)N = \left[F_{\dot{N}}^L(x), F_{\dot{N}}^U(x)\right] \subseteq [0,1]$ and

$$0 \leq \sup T_{\dot{N}}(x) + \sup I_{\dot{N}}(x) + \sup F_{\dot{N}}(x) \leq 3 \quad (4)$$

Let us consider some mathematical processes on IVNN (interval-valued neutrosophic numbers).

Definition2.4: Consider $\dot{N}_1 = \{< x : \left[T_{\dot{N}_1}^L, T_{\dot{N}_1}^U\right], \left[I_{\dot{N}_1}^L, I_{\dot{N}_1}^U\right],$

$\left[F_{\dot{N}_1}^L, F_{\dot{N}_1}^U\right] >, x \in X\}$ and $\dot{N}_2 = \{< x : \left[T_{\dot{N}_2}^L, T_{\dot{N}_2}^U(x)\right], \left[I_{\dot{N}_2}^L, I_{\dot{N}_2}^U\right]$

$$\delta\dot{N} = \langle [1 - (1 - T_N^L)^\delta, 1 - (1 - T_N^U)^\delta], \left[(T_N^L)^\delta, (T_N^U)^\delta\right], \left[(F_N^L)^\delta, (F_N^U)^\delta\right]\rangle \quad (5)$$

$$\dot{N}^\delta = \langle [(T_N^L)^\delta, (T_N^U)^\delta], [1 - (1 - I_N^L)^\delta, 1 - (1 - I_N^U)^\delta], [1 - (1 - F_N^L)^\delta, 1 - (1 - F_N^U)^\delta]\rangle. \quad (6)$$

Deneutrosophication formulations for IVNNs: To equate two. IVNNs N_1 and N_2. We utilize the score function (SF) that signifies a mapping from $[N(R)]$ into the actual line.

$$S_{Bolturk}(\dot{N}_1) = \left(\frac{(T_x^L + T_x^U)}{2} + \left(1 - \frac{(I_x^L + I_x^U)}{2}\right) * (I_x^U) - \left(\frac{(F_x^L + F_x^U)}{2}\right) * (1 - F_x^U)\right) \quad (7)$$

$$S_{Ridvan}(\dot{N}_1) = \left(\frac{1}{4}\right) \times (2 + T_x^L + T_x^U - 2I_x^L - 2I_x^U - F_x^L - F_x^U) \quad (8)$$

$$S_{Peng}(\dot{N}_1) = \left[\frac{2}{3} + \frac{(T_x^L + T_x^U)}{6} - \frac{(I_x^L + I_x^U)}{6} - \frac{(F_x^L + F_x^U)}{6}\right] \quad (9)$$

$$S_{Liu}(\dot{N}_1) = \left[2 + \frac{(T_x^L + T_x^U)}{2} - \frac{(I_x^L + I_x^U)}{2} - \frac{(F_x^L + F_x^U)}{2}\right] \quad (10)$$

$$S_{Harish}(\dot{N}_1) = \left(\frac{1}{8}\right)$$

$$\times [4 + (T_x^L + T_x^U - F_x^L - F_x^U - 2I_x^L - 2I_x^U)\,(4 - T_x^L - T_x^U - F_x^L - F_x^U)] \quad (11)$$

Definition2.5: Assume $S_N = \langle [S_T, S_I, S_M, S_E], (T_S, I_S, F_S)\rangle n$ as a TpNN then the precision, certainty, and score functions are computed below:

$$a(S_N) = COG(R) \times (T_S - F_S) \quad (12)$$

$$C(S_N) = COG(R) \times (T_S). \quad (13)$$

$$\mathbb{S}(S_N) = COG(R) \times \frac{(2 + T_S - I_S - F_S)}{3} \quad (14)$$

Definition2.6: Assume $R_N = \langle [R_T, R_I, R_P], (T_R, I_R, F_R)\rangle$ as a triangular neutrosophic number before the accuracy and score function were expressed below,

$$\mathbb{S}(R_N) = \frac{1}{12}[R_T + 2 \cdot R_T + R_P] \times [2 + T_R - I_R - F_R] \quad (15)$$

$$a(R_N) = \frac{1}{12}[R_T + 2 \cdot R_T + R_P] \times [2 + T_R - I_R + F_R]. \quad (16)$$

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

When $b = c$ in interval valued TpNN, then it turns into an interval valued triangular neutrosophic number.

C. Hyperparameter Tuning

Finally, the IWOA is applied for the IVNS method optimum hyperparameter tuning. WOA is a novel optimizer method based on the humpback whales. Humpback whales can encircle the prey once they have found the target. The WOA technique works based on the present optimum candidate solution being nearer to the optimal or the prey of interest. When the optimum search agent is chosen, the other search agents approach it. Using Eqs. (17) and (18), the whale behavior can be illustrated:

$$D = |C \cdot X^*(t) - X(t)| \tag{17}$$

$$X(t+1) = X^*(t) - A.D \tag{18}$$

In the equations, t is the existing iteration, A, and C are coefficient vectors, X^* refers to the optimum result location vector, X is the location vector, $||$ is the arbitrary value, and $\cdot$ is entry-wise multiplication. It is worth mentioning that if the best solution arises after all the cycles, X^* need to amend.

a) Exploitation Stage

To mathematically model humpback whale behavior in a bubble net, two strategies are generated:

1) Shrinking Encirclement Mechanism

Similar to GWO, the shrinking encirclement approach.

2) Spiral Location Updating

Initially, the distance among the whale at the position (X, Y) and the target at position (X^*, Y^*) is determined. Next, an equation of spiral is created among the whale's location and its victim to pretend the helix shaped humpback whales movements.

$$X(t+1) = D' \cdot exp^{bl} \cdot cos(2\pi l) + X^*(t) \tag{19}$$

In Eq. (19), D' is the distance between the i^{th} whales to the prey, a constant b shows defines the structure of a logarithmical spiral, l denotes a random integer within [1,1].

$$D' = |X^*(t) - X(t)| \tag{20}$$

Simultaneously, humpback whale swims in a spiral pattern and diminishing circle around the target. To characterize these behaviors, consider the spiral model to upgrade the whales' location or 50% probability of choosing the shrinking encircling approach.

b) Exploration Stage

Exploration is performed by a similar method based on the adjustment towards the vector A. Humpback whales often perform a random search based on the corresponding position. Thus, A with a random value higher than 1 or less than-l was used to strength the search agent to move out of the reference whales. The location of search agent is updated according to a random search agent at the exploration stage contrasted with the optimum search agent at the exploitation stage. If $|A| > 1$, then the exploration phase takes place, and the WOA technique performs a global search.

$$D = |C \cdot X_{rand}(t) - X(t)| \tag{21}$$

$$X(t+1) = X_{rand}(t) - A \cdot D \tag{22}$$

Here, X_{rand} refers to a random location vector selected from the existing population.

This technique decides the location update model according to the p value. The easiness of falling into the local optimum and weak global search ability are generated by the randomly generated number of p variable and the information that the WOA performs a global search at $p < 0.5$. These problems are tackled by the modifications recommended for WOA. The IWOA represents this adjustment. Parameter p can be replaced by the pp that dynamically changes based on the existing iteration t and maximum iteration $t_{\max}$.

$$pp = \frac{1}{(1 + exp^{(-t\max/t)})} - 0.4 \tag{23}$$

The location updating equation for the exploration and exploitation stages remains the same, with the single adjustment being the modification of the condition that triggers the activation of this method.

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

$$condition\ 1 = \begin{cases} p < 0.5 & \text{WOA} \\ p < pp & \text{IWOA'} \end{cases} \tag{24}$$

$$condition\ 2 = \begin{cases} p \geq 0.5 & \text{WOA} \\ p \geq pp & \text{IWOA} \end{cases} \tag{25}$$

The next adjustment is the shrinking behavior of a. In this work, A refers to the random integer within $[-a, a]$ whereas a is dropped from0 to 2 at iteration. Subsequently the behavior of A is defined by a value, k module is adding to the present adaptability of the model inclined towards the local or global optima.

$$a = \begin{cases} 2 - \dfrac{t^2}{k}, & if\ t < \dfrac{2k}{t} \\ \dfrac{2(t_{max} - t)^2}{t_{\max} - 2k}, & if\ \dfrac{2k^2}{t_{max}} < t \leq t_{\max} \end{cases} \tag{26}$$

Where k is strongly associated with the iteration counter t.

$$k = 0.6t^2 \tag{27}$$

The last adjustment is to present Differential Evolution (DE) to aid the problem of easily falling into the local optima and low search efficiency. This technique is used when the whale updates the location. The ρ value reduces as the iteration count increases. During the iteration, the present individual location is associated to the location attained after upgrading with the DE approach and takes the optimum location after and before the modification.

$$X(t+1) = rand(\quad) \cdot \left(X^*(t) - X(t)\right) + \varrho \cdot \left(X_{rand} - X(t)\right) \tag{28}$$

$$\varrho = 1 - \frac{e^{\frac{t}{t_{\max}}} - 1}{e - 1} \tag{29}$$

The IWOA develops an FF to acquire improved classifier performance. It identifies a positive integer to denote the best performance of the candidate solutions. In this research, the minimization of the classification rate of error is considered as the FF, as specified in Eq. (30).

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{no.of\ misclassified\ samples}{Total\ no.of\ samples} * 100 \tag{30}$$

4. Performance Validation

In this section, the performance validation study of the IVNSOA-IDS method is examined using CSE-CIC-IDS2018 dataset [19], which contains 17500 samples under seven classes are defined in Table 1. Attack Type: Web Attack (XSS, SQL Injection, Web), Brute Force (SSH, FTP), Botnet (Bot), Dos (SlowHTTPTest, Hulk, slowloris, GoldenEye), Infiltration (Infiltration), Benign, DDoS (LOIC-UDP, HOIC, LOIC-HTTP)

Table 1: Details on database

Classes	No. of Count
Benign	2500
DDoS	2500
Bot	2500
Brute Force	2500
Infiltration	2500
Dos	2500
Web Attack	2500
Total Count	17500

n Table 2 and Fig. 2, the classification results of the IVNSOA-IDS methodology under 80%TRAP:20%TESP and 70%TRAP:30%TESP. The table values implied that the IVNSOA-IDS algorithm has properly identified seven attacks samples. With 80%TRAP, the IVNSOA-IDS approach has gained average $accu_y$ of 98.73%, $prec_n$ of

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

95.57%, $reca_l$ of 95.57%, $F_{measure}$ of 95.56%, and AUC_{score} of 97.41%, respectively. Likewise, with 20%TESP, the IVNSOA-IDS process has obtained average $accu_y$ of 98.58%, $prec_n$ of 95.03%, $reca_l$ of 95.02%, $F_{measure}$ of 95.02%, and AUC_{score} of 97.10%, correspondingly. Followed by, with 70%TRAP, the IVNSOA-IDS method has gained average $accu_y$ of 98.07%, $prec_n$ of 93.25%, $reca_l$ of 93.27%, $F_{measure}$ of 93.25%, and AUC_{score} of 96.07%, respectively. Eventually, with 30%TESP, the IVNSOA-IDS technique has gained average $accu_y$ of 98.29%, $prec_n$ of 94.01%, $reca_l$ of 93.99%, $F_{measure}$ of 93.98%, and AUC_{score} of 96.50%, respectively.

Table 2: Classifier outcome of IVNSOA-IDS technique under various measures

Class	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$	AUC_{Score}
TRAP (80%)					
Benign	98.89	96.31	95.93	96.12	97.66
DDoS	98.56	94.61	95.41	95.01	97.25
Bot	98.63	94.71	95.75	95.22	97.43
Brute Force	99.09	96.31	97.33	96.82	98.36
Infiltration	98.84	95.62	96.24	95.93	97.75
Dos	98.70	96.43	94.40	95.40	96.91
Web Attack	98.42	94.99	93.90	94.44	96.54
Average	98.73	95.57	95.57	95.56	97.41
TESP (20%)					
Benign	98.51	93.75	95.68	94.70	97.33
DDoS	98.49	94.55	94.74	94.64	96.92
Bot	98.40	94.59	94.21	94.40	96.66
Brute Force	98.94	96.13	96.69	96.41	98.01
Infiltration	98.66	94.74	96.05	95.39	97.57
Dos	98.51	96.47	92.99	94.69	96.21
Web Attack	98.54	94.99	94.80	94.89	96.98
Average	98.58	95.03	95.02	95.02	97.10
TRAP (70%)					
Benign	97.62	91.77	91.67	91.72	95.14
DDoS	97.22	91.14	89.04	90.08	93.81
Bot	98.94	95.66	96.88	96.26	98.08
Brute Force	97.89	93.58	91.85	92.71	95.39
Infiltration	98.26	93.47	94.38	93.93	96.64
Dos	98.46	94.44	94.71	94.57	96.89
Web Attack	98.13	92.70	94.34	93.51	96.55
Average	98.07	93.25	93.27	93.25	96.07
TESP (30%)					
Benign	98.08	92.62	93.75	93.18	96.27
DDoS	97.50	93.32	89.31	91.27	94.11
Bot	98.97	95.67	97.41	96.53	98.33
Brute Force	97.96	93.61	91.10	92.34	95.07
Infiltration	98.42	92.75	96.56	94.61	97.64
Dos	98.48	95.10	94.35	94.72	96.76
Web Attack	98.63	94.97	95.47	95.22	97.31
Average	98.29	94.01	93.99	93.98	96.50

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

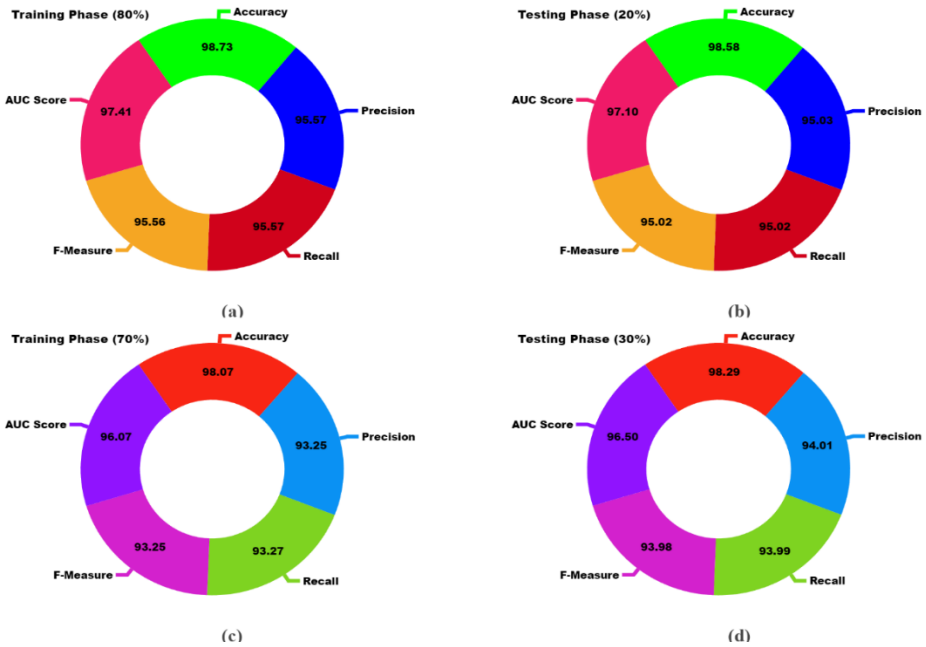

Figure 2. Average of IVNSOA-IDS technique (a-b) 80%TRAP:20%TESP and (c-d) 70%TRAP:30%TESP

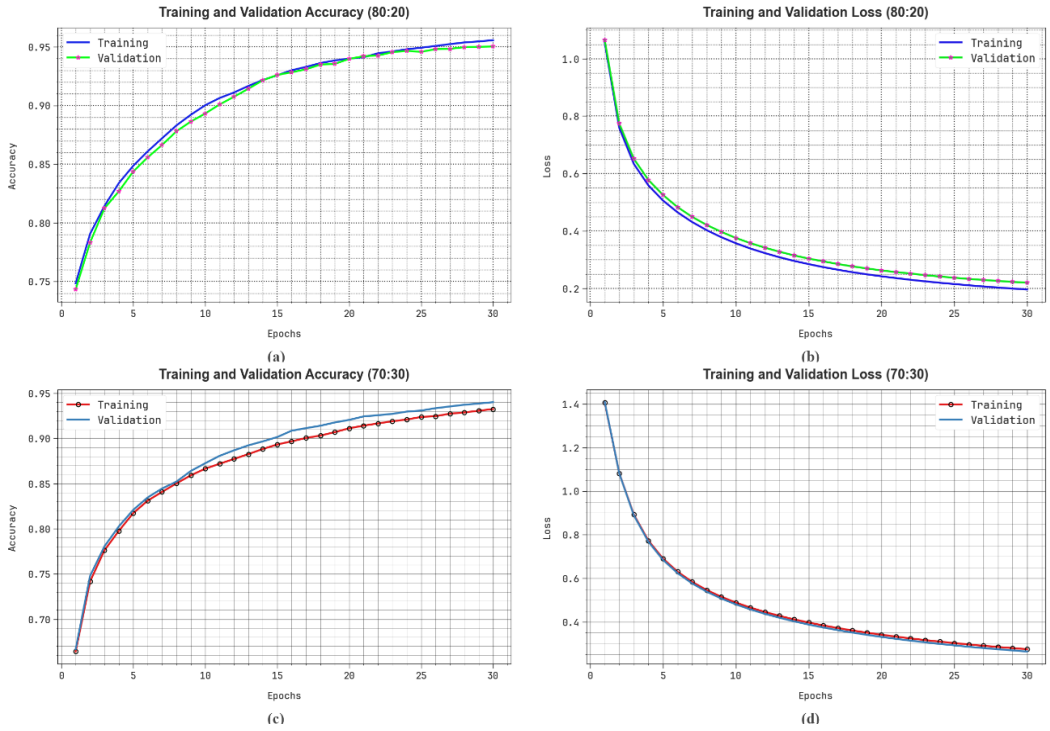

Figure 3. (a-c) Accuracy curve and (b-d) Loss curve

Fig. 3 displays the classification results of the IVNSOA-IDS system on 80%:20% and 70%:30%. Figs. 3a-3c represents the accuracy study of the IVNSOA-IDS methodology. The figure notifies that the CGOIDL-M IVNSOA-IDS model attains improve $accu_y$ values over increasing number of epochs. Also, the increasing validation (VLA) $accu_y$ over training (TRA) $accu_y$ show that the IVNSOA-IDS methodology learns proficiently. Finally, Figs. 3b-3d demonstrates the loss investigation of the IVNSOA-IDS approach. The outcomes display that the IVNSOA-IDS process attains closer outcomes of TRA and VLA loss. It is observed that the IVNSOA-IDS approach learns proficiently.

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

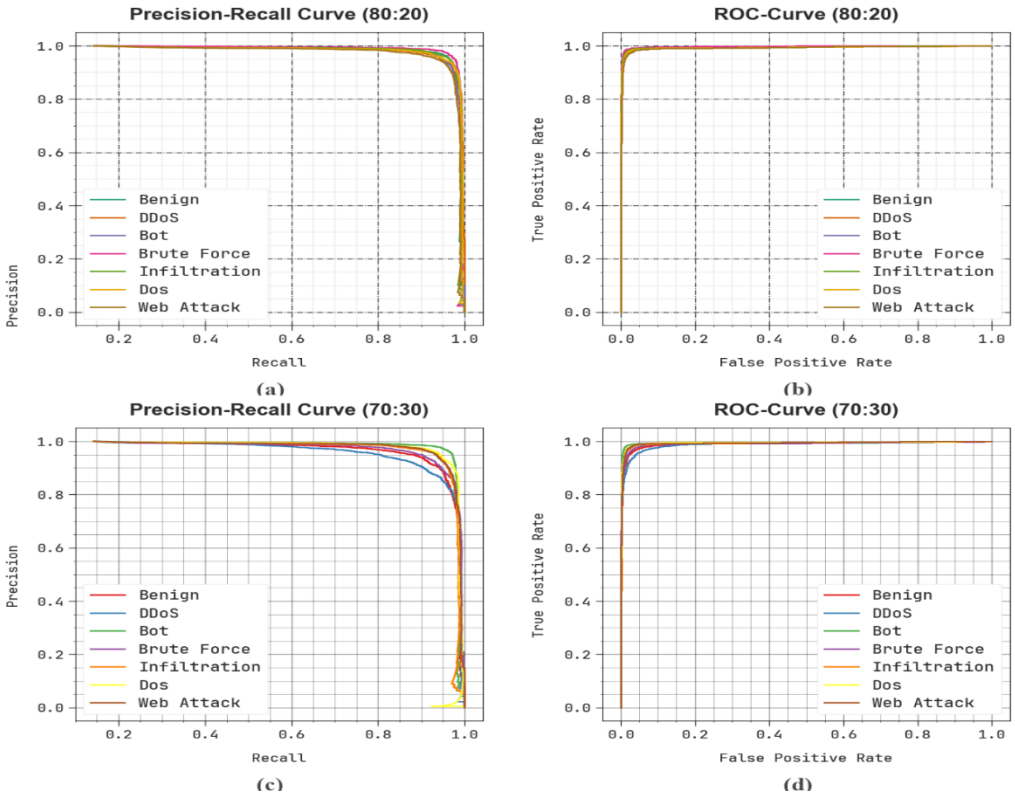

Figure 4. (a-c) PR curve and (b-d) ROC curve

Fig. 4 exhibits the classification results of IVNSOA-IDS process on 80%:20% and 70%:30%. Figs. 4a-4c illustrate the PR analysis of the IVNSOA-IDS system. The results indicated that the IVNSOA-IDS system outcomes in raising PR values. Furthermore, it is clear that the IVNSOA-IDS approach can attains higher PR values at 7 classes. Finally, Figs. 4b-4d displays the ROC investigation of the IVNSOA-IDS methodology. The figure defined that the IVNSOA-IDS process resulted to enhanced value of ROC. Moreover, it is evident that the IVNSOA-IDS model can extend enhanced value of ROC at 7 classes.

In Table 3 and Fig. 5, the experimental results of the IVNSOA-IDS process with recent models are given [20, 21]. The results shows that the RF model has shown worse performance with $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 93.17%, 91.68%, 89.65%, and 90.65%, correspondingly. At the same time, the MLP method has attained slightly increased outcomes with $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 94.50%, 93.45%, 93.53%, and 94.61%, correspondingly. Besides, the GoogLeNet, CNN, BayesNet, and logistic classifier has attained moderately closer performance. Meanwhile, the LogitBoost system has resulted in considerable results with$accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 98.20%, 92.04%, 93.16%, and 94.09%, respectively. But the IVNSOA-IDS approach outperforms the other models with maximum $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 98.73%, 95.57%, 95.57%, and 95.56%, correspondingly.

Table 3: Comparative outcome of IVNSOA-IDS technique with other existing methods

Techniques	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$
Random Forest	93.17	91.68	89.65	90.65
GoogLeNet	94.71	92.94	91.39	91.71
CNN Algorithm	95.92	93.62	92.10	92.34
BayesNet Model	96.50	92.98	92.94	94.80
Logistic Classifier	96.00	93.72	91.89	92.46
Multilayer perceptron	94.50	93.45	93.53	94.61
LogitBoost Model	98.20	92.04	93.16	94.09
IVNSOA-IDS	98.73	95.57	95.57	95.56

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

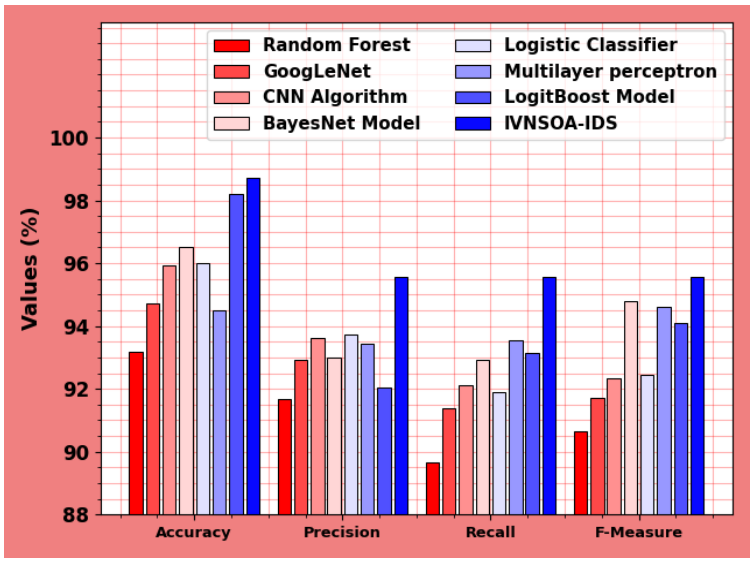

Figure 5. Comparative outcome of IVNSOA-IDS approach with existing techniques

5. Conclusion

In this research, we design a new IVNSOA-IDS technique in IoT cybersecurity. The key aim of the IVNSOA-IDS technique rests in the automatic identification of intrusion detection in IoT cybersecurity. It contains the three various processes involved in data pre-processing, classification, and hyperparameter tuning. Initially, the IVNSOA-IDS technique takes place when data pre-processing is executed to convert the raw data into a compatible format. Then, the IVNS classifier has been applied for the automated intrusion detection. Finally, the IWOA is employed for the optimum parameter tuning of the IVNS method. To demonstrate the enhanced performance of the IVNSOA-IDS technique, an extensive of simulations take place and the results are inspected under various aspects. The experimental validation analysis reported the advancement of the IVNSOA-IDS methodology under various metrics.

Funding: "This research received no external funding"

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

References

[1] Ibrahim, M.A., Agboola, A.A.A, Badmus, B.S., and Akinleye, S.A., "On Refined Neutrosophic Vector Spaces I", International Journal of Neutrosophic Science, Vol. 7, pp. 97-109, 2020.

[2] Smarandache F., and Abobala, M., " n-Refined Neutrosophic Vector Spaces", International Journal of Neutrosophic Science, Vol. 7, pp. 47-54, 2020.

[3] Tuqa A. H. Al-Tamimi, Luay A. A. Al-Swidi , Ali H. M. Al-Obaidi. "Partner Sets for Generalizations of MultiNeutrosophic Sets." International Journal of Neutrosophic Science, Vol. 24, No. 1, 2024 ,PP. 08-13

[4] Parimala, M., Karthika, M. and Smarandache, F., 2020. A review of fuzzy soft topological spaces, intuitionistic fuzzy soft topological spaces and neutrosophic soft topological spaces. International Journal of Neutrosophic Science, Vol. 10, No. 2, 2020 ,PP. 96-104.

[5] Ashraf, S. and Abdullah, S., 2020. Decision support modeling for agriculture land selection based on sine trigonometric single valued neutrosophic information. International Journal of Neutrosophic Science (IJNS), 9(2), pp.60-73.

[6] Alqahtani, H., Sarker, I.H., Kalim, A., Hossain, M., Md, S., Ikhlaq, S., & Hossain, S. (2020, March). Cyber intrusion detection using machine learning classification techniques. In International Conference on Computing Science, Communication and Security (pp. 121-131). Springer, Singapore.

[7] Shin, Y., & Kim, K. (2020). Comparison of anomaly detection accuracy of host-based intrusion detection systems based on different machine learning algorithms. International Journal of Advanced Computer Science and Applications, 11(2).

[8] Alzahrani, A.O., & Alenazi, M.J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Future Internet, 13(5), 111.

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024

[9] Rokade, M.D., & Sharma, Y.K. (2021, March). MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset. In 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 533-536). IEEE.

[10] Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2021). Practical real-time intrusion detection using machine learning approaches. Computer Communications, 34(18), 2227- 2235.

[11] Amoo, O.O., Osasona, F., Atadoga, A., Ayinla, B.S., Farayola, O.A. and Abrahams, T.O., 2024. Cybersecurity threats in the age of IoT: A review of protective measures. International Journal of Science and Research Archive, 11(1), pp.1304-1310.

[12] Ahakonye, L.A.C., Nwakanma, C.I. and Kim, D.S., 2024. Tides of Blockchain in IoT Cybersecurity. Sensors, 24(10), p.3111.

[13] Nadella, G.S. and Gonaygunta, H., 2024. Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT. International Journal of Science and Engineering Applications, 13(04), pp.30-33.

[14] Adewuyi, A., Oladele, A.A., Enyiorji, P.U., Ajayi, O.O., Tsambatare, T.E., Oloke, K. and Abijo, I., 2024. The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems. World Journal of Advanced Research and Reviews, 23(1), pp.379-394.

[15] Lai, T., Farid, F., Bello, A. and Sabrina, F., 2024. Ensemble learning based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis. Cybersecurity, 7(1), p.44.

[16] Maghrabi, L.A., Shabanah, S., Althaqafi, T., Alsalman, D., Algarni, S., Abdullah, A.L. and Ragab, M., 2024. Enhancing cybersecurity in the internet of things environment using bald eagle search optimization with hybrid deep learning. IEEE Access.

[17] Broumi, S., Nagarajan, D., Bakali, A., Talea, M., Smarandache, F. and Lathamaheswari, M., 2019. The shortest path problem in interval valued trapezoidal and triangular neutrosophic environment. Complex & Intelligent Systems, 5, pp.391-402.

[18] 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.

[19] https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv

[20] Najafi Mohsenabad, H. and Tut, M.A., 2024. Optimizing cybersecurity attack detection in computer networks: A comparative analysis of bio-inspired optimization algorithms using the CSE-CIC-IDS 2018 dataset. Applied Sciences, 14(3), p.1044.

[21] Yang, H., Xu, J., Xiao, Y. and Hu, L., 2023. SPE-ACGAN: A resampling approach for class imbalance problem in network intrusion detection systems. Electronics, 12(15), p.3323.

DOI: https://doi.org/10.54216/IJNS.250223
Received: March 22, 2024 Revised: May 11, 2024 Accepted: August 21, 2024