Integrating Machine Learning with Two-Person Intuitionistic Neutrosophic Soft Games for Cyberthreat Detection in Blockchain Environment

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

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

Abstract

Cyber-attacks involve a large number of malicious events including phishing, malware attacks, ransomware, social engineering, etc. Automatic cyber-attack recognition and classification are obtained by different technologies and techniques, including artificial intelligence (AI), data analytics, machine learning (ML), deep learning (DL), and other forward-thinking approaches. As a generality of the fuzzy set (FS) and intuitionistic FS (IFS), the Neutrosophic set (NS) can handle incongruous, uncertain, and indeterminacy data where the indeterminate is explicitly measured, and the degree of truth, indeterminacy, and false functions are liberated. It may successfully define inconsistent, uncertain, and incomplete data and overcome certain limitations of the present techniques in representing uncertain decision data. The indeterministic portion of uncertain information, presented in the NS concept, has been instrumented in proper decision-making that is impossible by the IFS concept. Cyber threat detection and classification is a crucial research area that develops intelligent systems that can identify and categorize a variety of cyber-attacks in real time. This article develops an Integrating Machine Learning with Two-Person Intuitionistic Neutrosophic Soft Games for Cyber threat Detection in Blockchain Environment (IMLTPIN-CDBE) system. The main aim of the IMLTPIN-CDBE methodology lies in the automatic recognition of the cyber-threat BC platform. The initial phase of data normalization using a min-max scalar is conducted in the IMLTPIN-CDBE method. Moreover, the two-person intuitionistic neutrosophic soft games (TPINSSG) technique is applied for cyberattack recognition. Finally, the grasshopper optimization algorithm (GOA) technique is applied for fine-tuning the hyperparameter included in the TPINSSG classifiers. A sequence of experiments has been conducted on the ransomware database to exhibit the great performance of the IMLTPIN-CDBE method. The empirical findings show the supremacy of the IMLTPIN-CDBE method over other current approaches.

Keywords: Cyberthreat Detection; Neutrosophic Soft Games, Grasshopper Optimization Algorithm; Fuzzy Set; Intuitionistic Fuzzy Sets

1. Introduction

The fuzzy set has been presented for dealing with unclear and undecided data. However, the fuzzy set was not the perfect technique, since it would be considered only truth membership and it failed to deal with the indeterminateness are regularly occurs in the real world [1]. Atanassov introduces an intuitionistic fuzzy set (IFS) as a continuation of FSs. The IFS and FSs failed to handle all kinds of uncertainty namely inconsistency and indeterminacy which frequently exist in the natural decision-making method [2]. According to these concepts, Smarandache suggested neutrosophic thinking, sets, and possibility. To promote the practicable part of the neutrosophic set, a single-valued neutrosophic set (SVNS) was presented [3]. In association with the developing scope of cyber threats, cyber-security also created a significant amount of developments to compete with opposing cyber offenses [4]. Cyber securities are a group of technology, technological specialists, and procedures which is utilized to create a safety measure for protecting cyberspace from cyber criminals [5]. Cyber-security contains two

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

major techniques such as automated cyber-security and conventional cyber-security. A cyber risk is considered to be an act in which somebody will attempt or try to purloin the data, disrupt the honesty guidelines, and damage the calculating devices or networks [6]. Cyber threats included attacks on IoT devices, malware, denial of service attacks, phishing, intrusion on a network or mobile devices, spam, ransomware, and financial fraud, to name a very few [7].

The following intrusions are employed to scan and detect the vulnerabilities of a computer system [8]. An intrusion detection system (IDS) is applied to defend against such intrusions. Blockchain (BC) presents an effective model for to fight against cyber risks. Because of this reason, numerous works were presented [9]. Nevertheless, as much as they know, they are mostly targeted for predicting various assaults. Analyzing huge information from hydrogenated devices could request a higher cognitive stack for improving efficient systems [10]. Additionally, these tasks expose the limits of ancient systems. Considering these limits and human nature, the pairing between AI and BC has been verified to challenge definitely with IIoT atmosphere [11]. The combination of deep learning (DL) models has considerably improved the effectiveness of the threat recognition system [12]. DL algorithms, mainly neural networks (NN), outshine mechanically in learning hierarchic demonstrations of information, allowing them to distinguish complicated patterns inside enormous data sets [13]. The application of recurrent neural network (RNN) and convolutional neural network (CNN) in tandem with behavioral scrutiny added to refine the precision of abnormality recognition, allowing securities systems to distinguish between usual changes and honestly malicious actions [14]. Considering machine learning (ML) algorithms proceed to improvement, the incorporation of explainability features becomes critical to improving the intelligibility of model conclusions, nurturing faith, and simplifying human mistakes in crucial security tasks [15].

This article develops an Integrating Machine Learning with Two-Person Intuitionistic Neutrosophic Soft Games for Cyberthreat Detection in Blockchain Environment (IMLTPIN-CDBE) model. The main aim of the IMLTPIN-CDBE approach lies in the automatic recognition of the cyber threat BC platform. The initial phase of data normalization using a min-max scalar is conducted in the IMLTPIN-CDBE method. Moreover, the two-person intuitionistic neutrosophic soft games (TPINSSG) technique is applied for cyberattack recognition. Finally, the grasshopper optimization algorithm (GOA) technique is applied for fine-tuning the hyperparameter included in the TPINSSG classifiers. The empirical findings show the supremacy of the IMLTPIN-CDBE method over other current approaches.

2. Related Works

Faheem and Al-Khasawneh [16] introduced big data sets achieved between the wind-power and the solar-circulated energy system by BC-based energy network in the Smart Grid (SG). A hybrid ML algorithm that merges both LSTM and DL models' features is established and useful to detect the novel design of Distributed Denial of Service (DDoS) and DoS cyber-attacks in the circulation method, transmission, and power generations. Jiang et al. [17] recommended a unique technique for threat intellect distribution named BC and Federated Learning to share (BFLS), a threat recognition method for Cyber Threat Intelligence (CTI) wherever BC-based CTI distribution bases were applied with privacy and security. Additionally, users may get highly qualified threat recognition models except for sending private information to the dominant servers. Zkik et al. [18] develop integrated artificial intelligence (AI) models for preventing anomaly detections and smart contract susceptibilities. Therefore, Graph Neural Networks (GNN) methods are extended for protecting BC-based crowd-funded bases from smart contracts-based assaults namely infinite loop attacks and re-entry. Therefore, ML techniques are utilized for anomaly recognition and to prevent assaults like DDoS assaults, malware, and progressive persistent attacks.

Albakri et al. [19] focus on the designs of BC-aided mixed meta-heuristics with ML-based Cyberattacks detections and classifications (BHMML-CADC) technique. This BHMML-CADC models use Ethereum BC for violence recognition. Additionally, the hybrid enhanced glow-worm swarm optimizer (HEGSO) method was employed for feature selection. Furthermore, Cyber-attacks could be recognized by designs of the quasi-recurrent neural networks (QRNNs) techniques. At Last, hunter–prey optimizer (HPO) algorithms are applied toward an optimal choice of the QRNN factors. In [20], a BC-based model is introduced for data safety in which blockages are made with the RSA hash technique. Applying Differential Evolution (DE), this method initially chooses the BC-ensured data, and then the method splits that information into trained and trial data sets to practice for testing and training the models. It also allowed us to validate the methods for using DBN to forecast assaults. Khan et al. [21] proposed to establish a unique may-fly optimization with a Regularized Extreme Learning Machine algorithm named MFO-RELM technique through Cyber security threat detections along with classifications with IoT and the cloud atmospheres. The MFO-RELM models pre-processed the real IoT and cloud information into an important form.

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

Further, the recommended model would obtain the preprocessing information and perform the classification methods. To boost the effectiveness of the suggested technique, the MFO algorithm has been applied to it.

3. The Proposed Model

In this paper, we designed a novel IMLTPIN-CDBE methodology. The main aim of the IMLTPIN-CDBE system lies in the automatic recognition of the cyber threat BC platform. The IMLTPIN-CDBE method comprises min-max scalar-based normalization, TPINSSG-based cyberattack detection, and GOA-based fine-tuning processes. Fig. 1 depicts the workflow of the IMLTPIN-CDBE technique.

A. Preprocessing using Min-Max Scalar

In the initial phase, the data normalization using a min-max scalar is conducted in the IMLTPIN-CDBE method. Min-max scaling is an indispensable data normalization method in cyberattack recognition, which rescales the features into the interval of 0 and 1 [22]. This ensures uniformity across various data dimensions, improving the performance of ML techniques. By removing differences in feature scales, min-max scaling enables efficient recognition of patterns and anomalies indicative of possible cyberattacks.

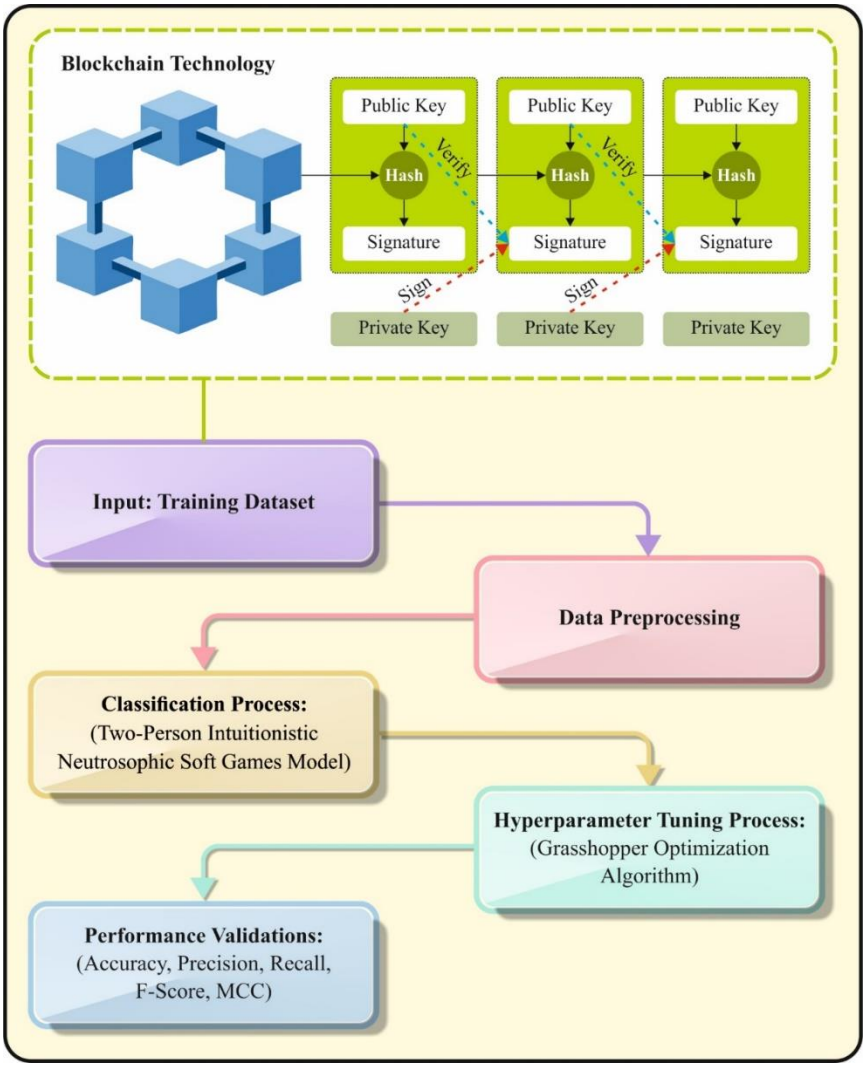

Figure 1. Workflow of IMLTPIN-CDBE technique

B. Cyberattack Detection Using TPINSSG Technique

At this phase, the classification of the Neutrosophic method deals with uncertainty and vagueness basic in illusive content recognition tasks [23]. In this section, we give some simple descriptions at first and next construct $Tp\text{-}ins\text{-}game$ with INS-payoff. We extend the idea of many game theory types into the INS game.

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

Description 3.1 Assume G as a plan set and, $Q \subseteq G$. next, the range of each ordered set $P \times Q$ is called available action sets.

Description 3.2 Assume U as an alternative set and IN^U signifies the range of every INS over U. While, G signifies a strategies sets i.e., $P, Q \subseteq G$. Next, the set value function $\rho_{P\times Q}: P \times Q \to lN^U$ is called a function of INS-payoff and determined as

Description 3.3 Assume $P \times Q$ as available action sets. The $(p^*, q^*) \in P \times Q$ action is called an optimal action if $\rho_{P\times Q}(p^*, q^*) \supseteq \rho_{P\times Q}(,q) i.e. \mu_T(p^*, q^*) \geq \mu_T(,q), \delta_I(p^*, q^*) \geq \delta_I(p,q),$ and $\gamma_F(p^*, q^*) \leq \gamma_F(p,q), \forall (p,q) \in P \times Q$.

Description 3.4 Assume $P \times Q$ as an available action set and $(p_i, q_j), (p_k, q_l) \in P \times Q$.

a) When $\rho_{P\times Q}(p_i, q_j) \supset \rho_{P\times Q}(p_\kappa, q_l)$, a player selects (p_i, q_j) over (p_k, q_l) or is moderate between the two actions.

b) When $\rho_{P\times Q}(p_i, q_j) \supset \rho_{P\times Q}(p_\kappa, q_l)$, then a player will select (p_i, q_j) over (p_k, q_l).

Description 3.5 While Q and P denote the set of strategies of players l and 2 respectively. U represents an alternative set and $p_{P\times Q}: P \times Q \to IN^U$ refers to a function of $INS\text{-}payoff$ for player's $k = 1,2$. Then, $Tp\text{-}ins\text{-}game$ has been chosen and diverse by an $INS\text{-}over\ U$ as

$$\gamma^k_{P\times Q} = \{((p,q)_t \rho_{P\times Q}(p,q)) : (p,q) \in P \times Q\}$$

We express $Tp\text{-}ins\text{-}game$ as at a correct period, the player 1 prefers an approach $p_i \in P_t$ simultaneously, player2 chooses another tactic $q_i \in Q$. Next, each player's $k = 1,2$ holds the

$INS - payoff\ \rho_{P\times Q}(p_i, q_j)$.

When $Q = \{q_1, q_2, \dots\dots\dots, q_s\}$ and $= \{p_1, p_2, \dots\dots\dots, p_r\}$, then the INS payoff $\rho^k_{P\times Q}$ is presented in the matrix method of $r \times s$.

Instance 3.6 Assume $U = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7\}$ as an alternative set and $E = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ as a set of strategies. While, IN^U indicates the set of each INS over U and $A = \{a_1, a_{32} a_5\}$ and $B = \{a_3, a_5\}$ denotes a set of strategies of Player l and Player 2, respectively.

If player l constructs the Tp-ins-game as follows,

$$\gamma^1_{A\times B} = \begin{Bmatrix} ((a_1, a_3), \{(0.5,0.4,0.3), u_1, (0.3,0.7,0.4)/u_3, (.2,0.6,0.4)/u_5\}), \\ ((a_1, a_5), \{(0.5,0.6,0.3)/u_2, (0.4,0.6,0.3)/u_{3t}(0.5,0.1,0.6)u_5 \\ ((a_3, a_3), \{(0.6,0.4,0.\cdot 4)/u_1, (0.1,0.6,0.3)/u_4, (0.5,0.5,0.6)/u_6\}), \\ ((a_3, a_5), \{(0.8,0.4,0.6)u_2, (0.3,0.9,0.5)/u_3, (0.8,0.5,0.4)/u_4\}) \\ ((a_5, a_3), \{(0.3,0.7,05)/u_2, (0.2,0.8,0.5)/u_3, (0.1_t 0.3_t 0.8)u_5\})_t \\ ((a_5, a_5), \{(0.7,0.3,05)/u_1, (0.2,0.5,0.7)/u_2, (0.4,0.8,0.5)/u_4\}) \end{Bmatrix}$$

We measured some game elements. If player l selects a_3 and player 2 picks a_5, then the value of game will be {(0.8,0/, (0.3,0.9,0/, (0.8,0.5,0/}, next the access at the row intersection by a_3 and column beside a_5. Similarly, if player 2 constructs the Tp-ins-game as follows,

$$b^2_{A\times B}$$

$$= \{\{^{(,a_3)_t\ \{(0.6,0.5,0.4), (0.7_t 0.3_t 0.5)/u_5\})_t ((a_{12} a_5)_t \{(0.6_t 0.4_t 0.3)/u_{22} (0.3_t 0.8_t 0.4)/u_{42} (0.2_t 0.1_t 0.4)/u_5\})}$$

$$B^2_{A\times B} = \begin{Bmatrix} ((a_1, a_3), \{(0.6,0.5,0.4)/u_3, (0.7,0.3,0.5)/\}), ((a_1, a_5), \{(0.6,0.4,0.3)/u_2, (0.3,0.8,0.4)/u_4, \\ (0.2,0.1,0.4)/u_5\}) \\ ((a_3, a_3), \{(0.5,0.4,0.4), (0.3,0.7,0.5)/u_5, (0.6,0.5,0.4)/u_6\}), ((a_3, a_5), \\ (0.4,0.8,0.4)/u_l (0.3,0.9,0.5)/u_3 (0.7,0.5,0.4)/u_5 \\ ((a_5, a_3), \{(0.2,0.6,0.5)u_3/u_2 (0.2,0.6,0.5)/u_4, (0.2,0.8,0.4)/u_5\}), ((x_5, x_5), \\ \{(0.8,0.4,0.5)/u_4, (0.4,0.5,0.8)/u_6, \}) \end{Bmatrix}$$

Description 3.7 The link of the players $INS\text{-}payoffs$ is an empty set.

Definition 3.8 Assume $\rho^k_{A\times B}$ as a function of INS-payoff of a - $ins\text{-}game\ y^k_{X\times Y}$, whereas $k = 1,2$.

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

Instance 3.9 Assume $U = \{u_1, u_2, u_3, u_4, u_5, u_6\}$ as a set of alternatives, $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2\}$ as a set of strategies of Player l and Player 2 respectively.

Now, $\cup_{i=1}^{3} \rho_{A\times B}^{k}(a_i, b_1) = \{(0.3,0.4,0.7)/u_1, (0.5,0.4,0.3)/u_2, (0.3,0.6,0.4)/u_3, (0.2_t 0.6_t 0.4)/u_5\}$

$\cup_{i=1}^{3} \beta_{A\times B}^{1}(a_i, b_2) = \{(0.7,0.4,0.5)/u_1, (0.5,0.6,0.3)/u_2, (0.4,0.9,0.3)/u_3, (0.8,0.8,0.4)/u_4, (0.3,0.6,0.3)/u_5\}$
Similarly,

$$\bigcap_{j=1}^{2} \rho_{A\times B}^{1}(a_1, b_j) = \{(0.3,0.4,0.7)/u_1, (0.5,0.4,0.3)/u_2, (0.3,0.6,0.4)/u_3, (0.2,0.6,0.4)/u_5\}$$

$$\bigcap_{j=1}^{2} \rho_{A\times B}^{1}(a_2, b_j) = \{(0.5,0.4,0.6)/u_2\}\, j = 1 \cap^2 \rho_{A\times B}^{1}(a_1, b_j) = \{(0.3,0.3,0.7)/u_1\}$$

Since, the intersection of the first row $\{(0.3{,}00\ lu_1, (0.5{,}0\ lu_2, (0.3,0.6,0.4)$, value of Tp-ins-game. So $\{(0.3{,}00/u$ the Tp-ins-game.

While the first-row intersection is equal to the first-column union. Therefore $\{(0.3,04,0.7)/, (0.5,04,0.3)/ , (0.3,06,04)/, (02,0.6,04)/\}$ denotes a value of INS saddle point. Therefore $\{(0.3,04,0.7)/, (0.5,04,0.3)/ , (0.3,06,04)/, (02,0.6,04)/\}$ refers to the value of $Tp\text{-}ins\text{-}game$. For example, if we swap $\{(0.2,0.4,0.7)/ , (0.5,0.4,0.3)/\}$ by $\{(0.2,0.4,0.7)/, (0.6,0.3,0.4)\}$, then a value of INS-saddle point won't be prevalent. Hence, the value of the game can't be created.

Description 3.10 Assume $y_{A\times B}$ as a Tp-ins-game with its equal INS-payoff function $\rho_{A\times B}$, where $p_{A\times B}(a,b) = \{(\mu_T(a,b), \delta_I(a,b), \gamma_F(a,b)) : \forall (a,b) \in A \times B\}$. Then,

(i) An INS-upper value was expressed as

$v^* = \{\cap_{b\in B}^{n}(\cup_{a\in A}^{n} p_{A\times B}(a,b)\} = \{(\cap_{b\in B}^{n}(\cup_{a\in A}^{n} \mu_T(a,b)\}, \cap_{b\in B}^{n}(\cup_{a\in A}^{n} \delta_I(a,b)), \cup_{b\in B}^{n}(\cap_{a\in A}^{n} \gamma_F(a,b))\}y$

(ii) An INS-lower value was signified as

$$v^* = \{\bigcup_{a\in A}^{n}(\bigcap_{b\in B}^{n} \rho_{A\times B}(a,b))\}$$
$$= \left\{\left(\bigcup_{a\in A}^{n}(\bigcap_{b\in B}^{n} \mu_T(a,b)\right), \bigcup_{a\in A}^{n}(\bigcap_{b\in B}^{n} \delta_I(a,b)\right), \bigcap_{a\in A}^{n}(\bigcup_{b\in B}^{n} \gamma_F(a,b))\}$$

(iii) When $v^* = v_*$ i.e. INS-lower and upper values of a Tp-ins-game are equal and called Tp-ins-game values that selected as $v^* = v_* = v$.

Description 3.12 Assume $y_{A\times B}^{k}$ as a Tp-ins-game with its function of INS-payoff $\rho_{A\times B}^{k}$ for $k = 1{,}2$.

(i) $\rho_{A\times B}^{1}(a^*, b^*) \supseteq \rho_{A\times B}^{1}(a, b^*)$, for each $a \in A$

$(ii)\rho_{A\times B}^{2}(a^*, b^*) supseteq \rho_{A\times B}^{2}(a^*, b)$, for each $b \in B$

then, $(a^*, b^*) \in A \times B$ is called the INS-Nash balance of a Tp-ins-game.

C. Hyperparameter Tuning employing GOA

Finally, the GOA technique is applied for fine-tuning the hyperparameter included in the TPINSSG classifiers. GOA is a meta-heuristic technique, which reproduces grasshopper swarm-searching behavior [24]. Many grasshoppers cause catastrophic farming damage.

Eggs inlay into nymphs. A nymph is nothing but a grasshopper without wings. Short, sluggish mobility and small stages mark this period of grasshopper life. The grasshopper nymph develops in several days. Different nymphs and adults drive fast and far. These 2 nymph and grasshopper motions signify a meta-heuristic technique of exploitation and exploration. It is also optimum food source hunting skills. Food-searching behavior, grasshopper and nymph motions are mathematical formulated below:

$$X_i = S_i + G_i + A_i \tag{1}$$

During this case, the grasshopper social contact is represented by S_i in Eq. (2), i^{th} grasshopper location is signified by X_i, i^{th} grasshopper's force of gravity is denoted by G_i and wind advection is A_i. By adjusting Eq. (1), randomized has been combined into the performance of $grasshoppers X_i = r_i S_i + r_2 G_i + r_3 A_i$, they range between zero and one.

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

$$S_{ij} = \sum_{j=1, j\neq i}^{N} s\left(d_{ij}\right)\hat{d} \tag{2}$$

$$s(r) = fe^{\frac{-r}{l}} - e^{-r} \tag{3}$$

whereas the attractive length scale is signified as 1, attraction intensity is implied as f These 2 features define grasshopper repulsion, attraction, and comfort zones. Fixed $l = 1.5$ and $f = 0.5$.

$$G_i = -g \times \hat{e}_g \tag{4}$$

$$A_i = u \times \hat{e}_w \tag{5}$$

If S, G, and A modules of Eq. (1) are replaced, it develops:

$$X_i = \sum_{j=1, j\neq i} s\left(\left|x_j - x_i\right|\right)\frac{x_j - x_i}{d_{ij}} - g\hat{e}_g + u\hat{e}_w \tag{6}$$

whereas N refers to the count of Grasshoppers.

The swarm method was employed in free space. Eq. (6) has been utilized for simulating a connection among the group of grasshoppers. Figure 2 depicts the steps involved in GOA.

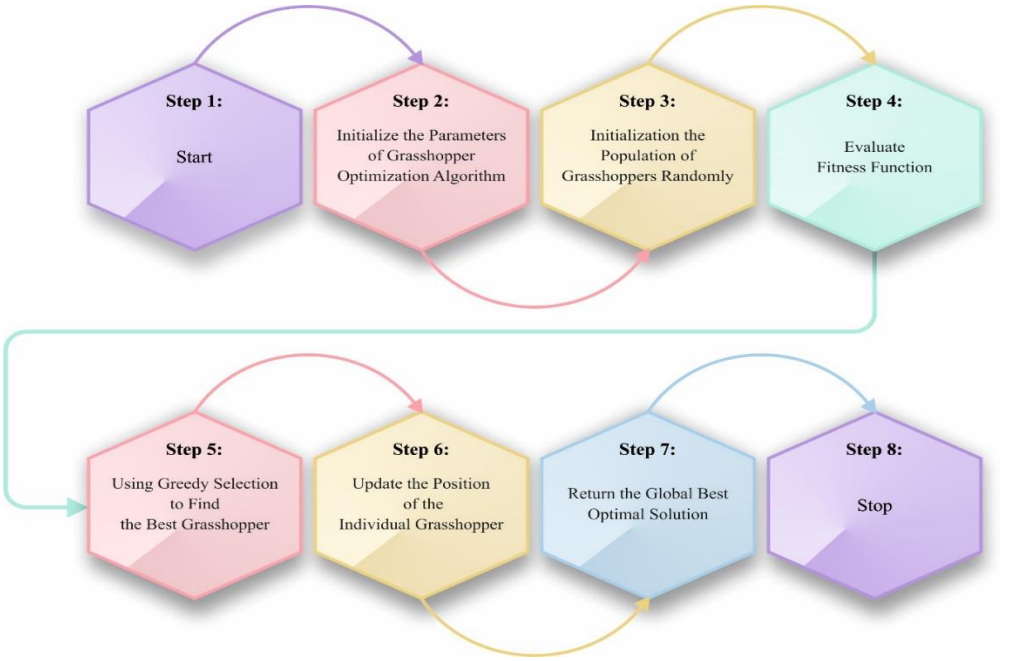

Figure 2. Steps involved in GOA

The selection of fitness is the significant factor manipulating the efficiency of GOA. The hyperparameter selection procedure includes the solution-encoded method to assess the efficiency of the candidate solution. In this paper, the GOA reflects accuracy as the main standard for proposal FF, which is expressed below.

$$Fitness = \max(P) \tag{7}$$

$$P = \frac{TP}{TP + FP} \tag{8}$$

Where TP is the value of true positive and FP denotes the value of false positive.

4. Experimental Validation

The experimental validation outcomes of the IMLTPIN-CDBE method are verified utilizing the CICIDS-2017 dataset [25]. The dataset comprises 10973 samples with five classes as shown in Table 1.

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

Table 1: Details on Dataset

CICIDS-2017 Dataset	
Classes	No. of Samples
Benign	2500
DDoS	2500
DoS	2500
Bot	1966
Web Attack	1507
Total Samples	10973

In Table 2, the overall recognition outcomes of the IMLTPIN-CDBE method are inspected in several epochs. The IMLTPIN-CDBE technique properly recognized five distinct attacks. With 500 epochs, the IMLTPIN-CDBE system got an average of $accu_y$ of 99.27%, $prec_n$ of 98.13%, $reca_l$ of 98.08%, F_{score} of 98.10%, and MCC of 97.65%. Besides, with 1000 epochs, the IMLTPIN-CDBE method got an average of $accu_y$ of 99.91%, $prec_n$ of 99.77%, $reca_l$ of 99.80%, F_{score} of 99.79%, and MCC of 99.73%. Followed by, with 1500 epochs, the IMLTPIN-CDBE method achieved an average of $accu_y$ of 99.39%, $prec_n$ of 98.42%, $reca_l$ of 98.50%, F_{score} of 98.46%, and MCC of 98.08%. Likewise, with 2000 epochs, the IMLTPIN-CDBE technique reached an average of $accu_y$ of 99.52%, $prec_n$ of 98.79%, $reca_l$ of 98.81%, F_{score} of 98.80%, and MCC of 98.50%. In addition, with 2500 epochs, the IMLTPIN-CDBE model got an average of $accu_y$ of 99.42%, $prec_n$ of 98.54%, $reca_l$ of 98.50%, F_{score} of 98.52%, and MCC of 98.16%. Lastly, with 3000 epochs, the IMLTPIN-CDBE approach reached an average of $accu_y$ of 99.07%, $prec_n$ of 97.60%, $reca_l$ of 97.62%, F_{score} of 97.61%, and MCC of 97.02%.

Table 2: Classifier outcome of IMLTPIN-CDBE technique under dissimilar epochs

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
Epoch - 500					
Benign	99.26	98.63	98.12	98.38	97.90
DDoS	99.23	98.40	98.20	98.30	97.80
DoS	99.42	98.80	98.64	98.72	98.34
Bot	99.13	96.43	98.83	97.61	97.10
Web Attack	99.32	98.38	96.62	97.49	97.10
Average	99.27	98.13	98.08	98.10	97.65
Epoch - 1000					
Benign	99.93	99.96	99.72	99.84	99.79
DDoS	99.94	99.84	99.88	99.86	99.82
DoS	99.85	99.84	99.52	99.68	99.59
Bot	99.86	99.34	99.90	99.62	99.54
Web Attack	99.98	99.87	100.00	99.93	99.92
Average	99.91	99.77	99.80	99.79	99.73
Epoch - 1500					
Benign	99.44	98.96	98.60	98.78	98.42
DDoS	99.21	97.78	98.76	98.27	97.76
DoS	99.40	99.27	98.08	98.67	98.29
Bot	99.43	98.47	98.32	98.40	98.05
Web Attack	99.50	97.64	98.74	98.19	97.90
Average	99.39	98.42	98.50	98.46	98.08
Epoch - 2000					
Benign	99.46	98.53	99.12	98.82	98.48
DDoS	99.37	99.23	98.00	98.61	98.21
DoS	99.50	98.84	98.96	98.90	98.58
Bot	99.59	98.44	99.29	98.86	98.61
Web Attack	99.67	98.94	98.67	98.80	98.61

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

Average	99.52	98.79	98.81	98.80	98.50
Epoch - 2500					
Benign	99.43	98.60	98.88	98.74	98.37
DDoS	99.37	98.64	98.60	98.62	98.21
DoS	99.35	98.68	98.48	98.58	98.16
Bot	99.43	98.13	98.73	98.43	98.08
Web Attack	99.52	98.66	97.81	98.23	97.96
Average	99.42	98.54	98.50	98.52	98.16
Epoch - 3000					
Benign	99.07	97.96	97.96	97.96	97.36
DDoS	98.98	97.91	97.60	97.76	97.10
DoS	98.98	97.87	97.64	97.76	97.10
Bot	99.13	97.22	97.97	97.59	97.07
Web Attack	99.17	97.01	96.95	96.98	96.50
Average	99.07	97.60	97.62	97.61	97.02

In Figure 3, the training and validation accuracy outcomes of the IMLTPIN-CDBE technique are established. The accuracy values are calculated over a range of 0-25 epochs. The outcome highlighted that the training and validation accuracy values display a rising tendency which reported the skill of the IMLTPIN-CDBE technique with enhanced performance over several iterations. Additionally, the training accuracy and validation accuracy remain closer over the epochs, which indicates low minimal overfitting and exhibits improved performance of the IMLTPIN-CDBE method, guaranteeing consistent prediction on hidden samples.

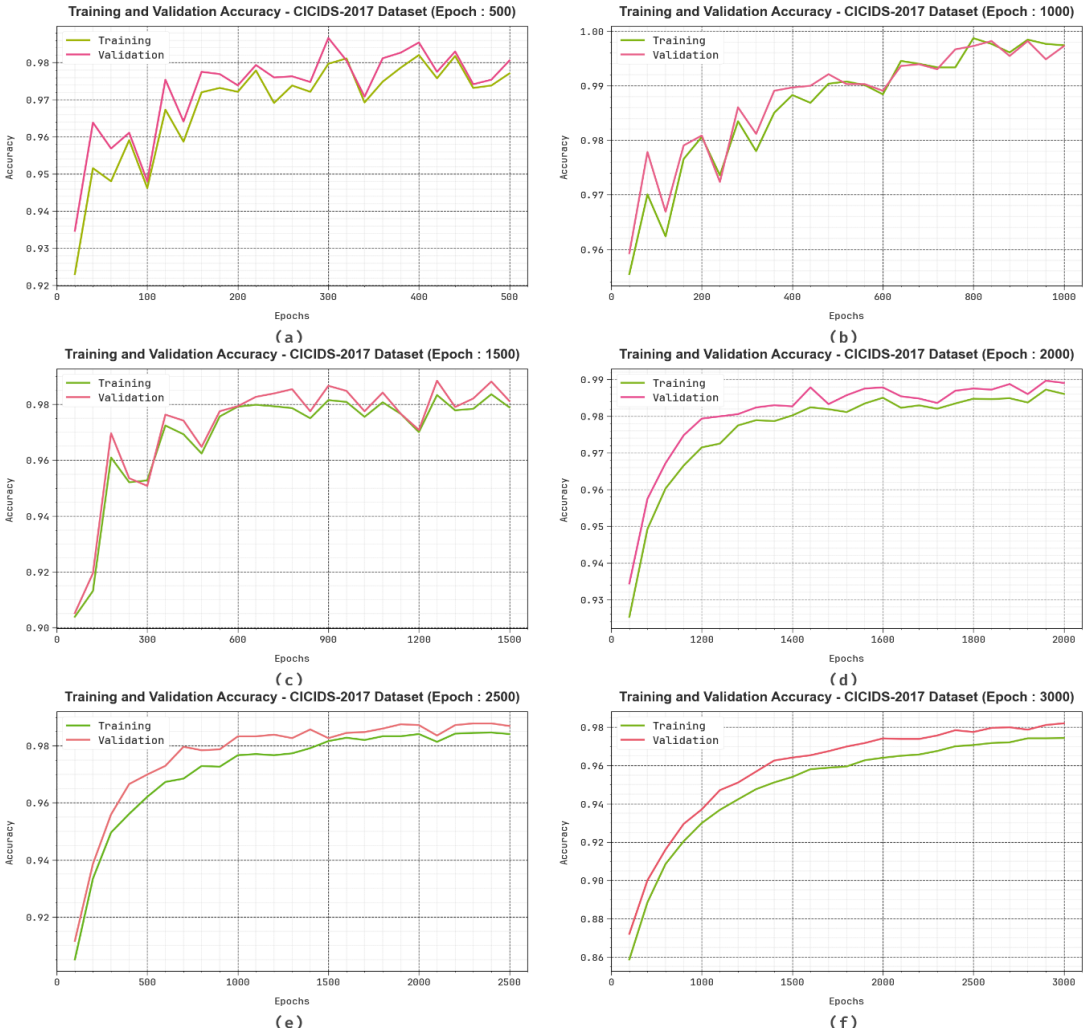

Figure 3. $Accu_y$ curve of IMLTPIN-CDBE technique (a-f) Epochs 500-3000

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

In Figure 4, the training and validation loss graph of the IMLTPIN-CDBE system is displayed. The loss values are calculated over a range of 0-25 epochs. It is signified that the training and validation accuracy values demonstrate a declining tendency, alerting the ability of the IMLTPIN-CDBE technique to balance a trade-off between data fitting and generalization. The continual decrease in loss values as well as assurances the heightened performance of the IMLTPIN-CDBE technique and tune the prediction outcomes over time.

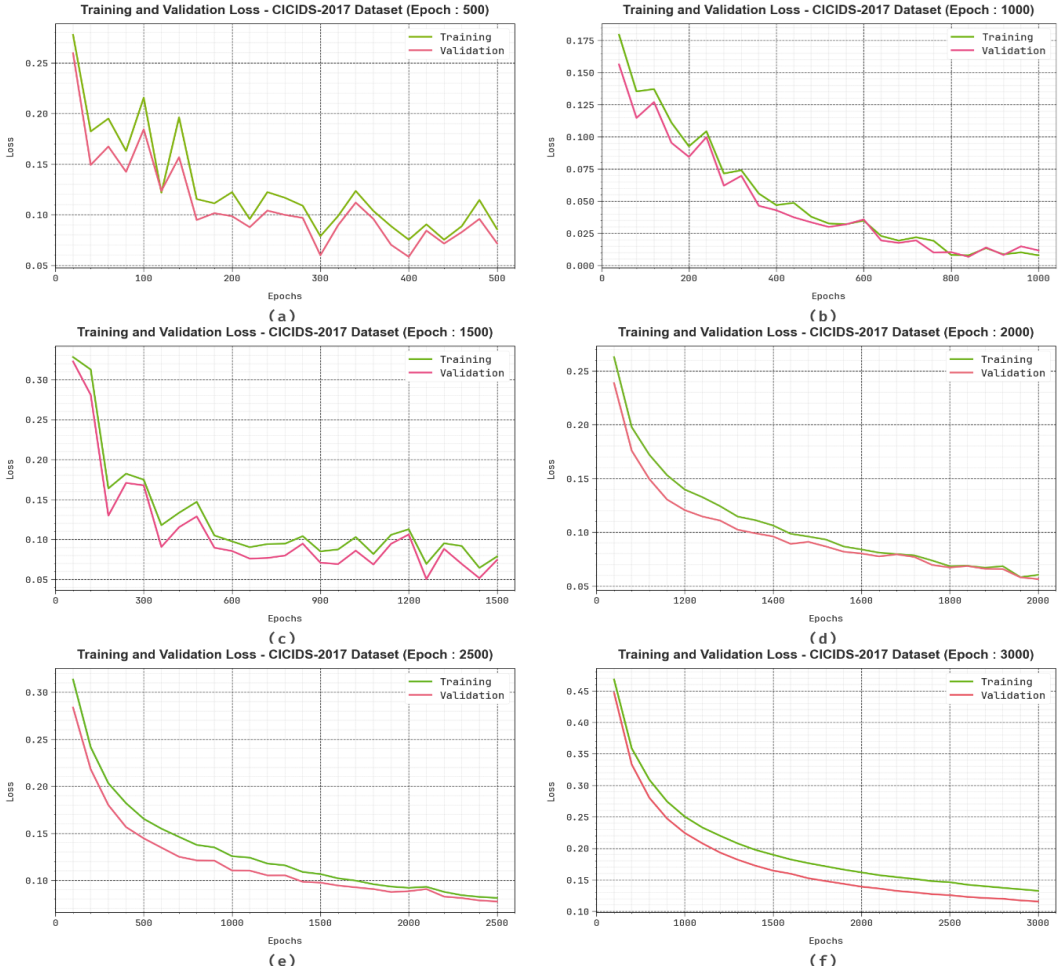

Figure 4. Loss curve of IMLTPIN-CDBE technique (a-f) Epochs 500-3000

To demonstrate the better performance of the IMLTPIN-CDBE method, a brief comparison study is prepared in Table 3 and Figure 5. The outcomes exemplified that the LightGBM and XGBoost models have shown lower classification results with $accu_y$ of 99.11% and 99.39%. In the meantime, the DT, RF, and Extra Tree models have tried to accomplish somewhat closer classification outcomes with $acccu_y$ of 99.48%, 99.39%, and 99.58%. Furthermore, the AdaBoost M and CIDH-ODLIDS models have exhibited reasonable performance with $accu_y$ of 99.65% and 99.77%. However, the IMLTPIN-CDBE technique demonstrates promising performance with $accu_y$ of 99.91%.

Table 3: Comparative analysis of IMLTPIN-CDBE method with other models

CICIDS-2017 Dataset	
Models	$\boldsymbol{Accu_y}$ (%)
IMLTPIN-CDBE	99.91
CIDH-ODLIDS	99.77
DT	99.48
RF	99.39

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

Extra Tree	99.58
AdaBoost M	99.65
LightGBM	99.11
XGBoost	99.39

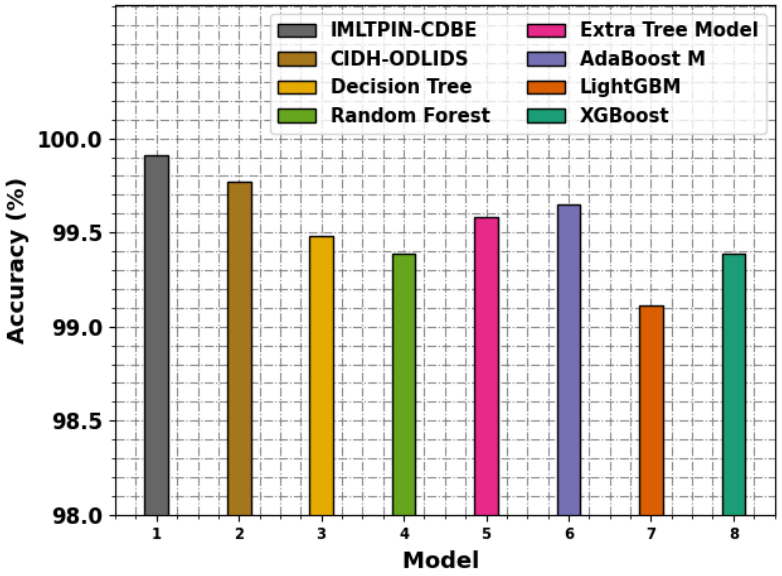

Figure 5. $Accu_y$ outcome of IMLTPIN-CDBE system with other approaches

5. Conclusion

In this paper, we have developed a novel IMLTPIN-CDBE model. The objective of IMLTPIN-CDBE method lies in the automatic detection of the cyber threat BC platform. The initial phase of data normalization using a min-max scalar is conducted in the IMLTPIN-CDBE method. Moreover, the TPINSSG technique is applied for cyberattack recognition. Finally, the GOA system was applied for fine-tuning the hyperparameter included in the TPINSSG classifiers. A sequence of experiments has been conducted on the ransomware database to exhibit the great performance of the IMLTPIN-CDBE method. The empirical findings show the supremacy of the IMLTPIN-CDBE method over other current approaches.

Funding: "This research received no external funding"

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

References

[1] Dhanalakshmi, G., Sandhiya, S. and Smarandache, F., 2024. Selection of the best process for desalination under a Treesoft set environment using the multi-criteria decision-making method. International Journal of Neutrosophic Science, 23(3), pp.140-40.

[2] Almuhur, E., Miqdad, H., Al-labadi, M. and Idrisi, M.I., 2024. μ-L-Closed Subsets of Noetherian Generalized Topological Spaces. International Journal of Neutrosophic Science, 23(3), pp.148-48.

[3] Tashtemirovich, A.O., Balba, M.E., Ibrohimjon, F. and Batirova, N., Investigating the Impact of Artificial Intelligence on Digital Marketing Tactics Strategies Using Neutrosophic Set.

[4] Sivakumar, C., Al-Qadri, M.O., Alsaraireh, A.A., Al-Husban, A., Meenakshi, P.M., Rajesh, N. and Palanikumar, M., 2024. q-rung square root interval-valued neutrosophic sets with respect to aggregated operators using multiple attribute decision making. International Journal of Neutrosophic Science, 23(3), pp.154-54.

[5] Gharib, M., Fakhry, A.E., Ali, A.M., Abdelhafeez, A. and Elbehiery, H., 2024. Single Valued Neutrosophic Sets for Analysis Opinions of Customer in Waste Management. International Journal of Neutrosophic Science, 23(3), pp.184-84.

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024

[6] Purohit, S., Calyam, P., Wang, S., Yempalla, R. and Varghese, J., 2020, September. Defensechain: Consortium blockchain for cyber threat intelligence sharing and defense. In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 112-119). IEEE.

[7] Gong, S. and Lee, C., 2020. Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance. Electronics, 9(3), p.521.

[8] Homan, D., Shiel, I. and Thorpe, C., 2019, June. A new network model for cyber threat intelligence sharing using blockchain technology. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-6). IEEE.

[9] Porkodi, S. and Kesavaraja, D., 2022. Intelligence on Situation Awareness and Cyberthreats Based on Blockchain and Neural Network. In Applications of Blockchain and Big IoT Systems (pp. 101-131). Apple Academic Press.

[10] Madaan, G., Bhushan, B. and Kumar, R., 2021. Blockchain-based cyberthreat mitigation systems for smart vehicles and industrial automation. Multimedia technologies in the Internet of Things environment, pp.13-32.

[11] 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.

[12] Habib, S., Alsanea, M., Aloraini, M., Al-Rawashdeh, H.S., Islam, M. and Khan, S., 2022. An efficient and effective deep learning-based model for real-time face mask detection. Sensors, 22(7), p.2602.

[13] 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.

[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] Dornadula, V.N. and Geetha, S., 2019. Credit card fraud detection using machine learning algorithms. Procedia computer science, 165, pp.631-641.

[16] Faheem, M. and Al-Khasawneh, M.A., 2024. Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. Data in Brief, 54, p.110461.

[17] Jiang, T., Shen, G., Guo, C., Cui, Y. and Xie, B., 2023. BFLS: Blockchain and Federated Learning for sharing threat detection models as Cyber Threat Intelligence. Computer Networks, 224, p.109604.

[18] Zkik, K., Sebbar, A., Fadi, O., Kamble, S. and Belhadi, A., 2024. Securing blockchain-based crowdfunding platforms: an integrated graph neural networks and machine learning approach. Electronic Commerce Research, 24(1), pp.497-533.

[19] Albakri, A., Alabdullah, B. and Alhayan, F., 2023. Blockchain-assisted machine learning with hybrid metaheuristics-empowered cyberattack detection and classification model. Sustainability, 15(18), p.13887.

[20] Aljabri, A., Jemili, F. and Korbaa, O., 2024. Intrusion detection in cyber-physical system using rsa blockchain technology. Multimedia Tools and Applications, 83(16), pp.48119-48140.

[21] Khan, Z.F., Alshahrani, S.M., Alghamdi, A.A., Alangari, S., Altamami, N.I., Alissa, K.A., Alazwari, S., Al Duhayyim, M. and Al-Wesabi, F.N., 2023. Machine Learning Based Cybersecurity Threat Detection for Secure IoT Assisted Cloud Environment. Comput. Syst. Sci. Eng., 47(1), pp.855-871.

[22] Deepa, B. and Ramesh, K., 2022. Epileptic seizure detection using deep learning through min max scaler normalization. Int. J. Health Sci, 6, pp.10981-10996.

[23] Mahzari, M., Hashim, A.H.A., Saeed, K.M.O. and Mokhtar, M.M.O., 2024. Two-Person Intuitionistic Neutrosophic Soft Games with Harris Hawks Optimizer based Tweets Classification on NLP Applications. Full Length Article, 24(1), pp.314-14.

[24] Gupta, R., Singh, P., Alam, T. and Agarwal, S., 2023. A deep neural network with hybrid spotted hyena optimizer and grasshopper optimization algorithm for copy move forgery detection. Multimedia Tools and Applications, 82(16), pp.24547-24572.

[25] https://www.unb.ca/cic/datasets/ids-2017.html

DOI: https://doi.org/10.54216/IJNS.250204
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 23, 2024