IDLTM-DMT: Intelligent Deep Learning based Trust Management with Decision Making Tool for Healthcare Internet of Things and Big Data Environment with Neutrosophic Set Analysis

C. K. Marigowda[1,*], Thriveni J.[2], Gowrishankar S.[3]

[1]Department of Information Science and Engineering, Acharya Institute of Technology, Visvesvaraya Technological University, Bengaluru-560107, India

[2]Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bengaluru-560001, India

[3]Department of Machine Learning, B M S College of Engineering, Bengaluru-560019, India

Emails: marigowda@acharya.ac.in; drthrivenij@gmail.com; gowrishankar.cse@bmsce.ac.in

Abstract

Over the last few years development of Internet of Things (IoT) devices and communication technologies have resulted in the massive generation of health-related data. In the context of healthcare, IoT offers several advantages, including being able to observe patients very closely and using data for analytics. A major challenging issue that exists in the usage of IoT and big data in the medical field is security. As healthcare data is highly vulnerable and becomes a target for attacks, there are significant privacy issues related to the usage of big data analytics. Besides, implementing new data analysis tools and strategies for handling big data decision-making is a major issue. The capability to examine this amount of data is a significant aspect of big data in health care. For resolving these issues, this paper presents a new intelligent deep learning-based trust management with decision making tool (IDLTM-DMT) for IoT healthcare big data environments, incorporating Neutrosophic Set Analysis (NSA). The proposed IDLTM-DMT model enables IoT devices to gather healthcare data. The IDLTM-DMT model involves a DL based bidirectional long short-term memory (BiLSTM) model for vulnerability detection and thereby identifies the malicious traffic in the Network. Hadoop MapReduce is used for handling big data and a decision-making tool using Deep Stacked Auto Encoder (DSAE) is used for the classification of diseases that exist in big data. To optimize the DSAE model's hyperparameters and improve classification performance, the Sandpiper Optimization (SPO) Algorithm is employed. Neutrosophic Set Analysis is integrated to manage the indeterminacy and inconsistency of the data, enhancing the decision-making process. Extensive experimental analysis is conducted on the EEG Eye State Dataset, with results analyzed using various performance measures. The findings indicate that the proposed method achieves improved accuracy compared to existing methods, demonstrating the effectiveness of incorporating Neutrosophic Set Analysis in IoT healthcare big data environments.

Keywords: Big data; Trust; Security; Internet of Things; Neutrosophic Set; Deep learning; Healthcare; Vulnerability Detection

1. Introduction

Presently, the Internet of things (IoT) is used in several healthcare fields to analyze real world data and recommendations accordingly. It plays a significant part in applications specially that involves global sensor and actuator interacting via wireless sensor network (WSN) toward the solution of several challenges. Most

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

applications nowadays have high demand for processing faster of produced data [1]. Moreover, several problems arise like data variation, volume, and velocity because of the usage of mobility, sensor, and geographic distribution as well as necessities for security, accuracy, operation cost, and quality of service (QoS). Fig. 1 shows the trust model of IoT system [2].

Recently, cloud computing (CC) technique was broadly implemented in IoT allowed healthcare applications for providing reliability, scalability, and data analyses. The geographical distribution of cloud data centre process data gathered from sensor needs communication via multi hop distance influxes the delay sensitive healthcare application. Furthermore, healthcare application platforms are diverse in nature, hence administration the cloud of resources allocation for uncertain and uneven data load comes in healthcare solution is a highly difficult process. Big data is deliberated as a huge number of semi structured, unstructured, and structure data that are always received and generated via hospitals. Based on present organization's understanding, method for handling bigdata is to employ analysis for their big data and attain beneficial perceptions.

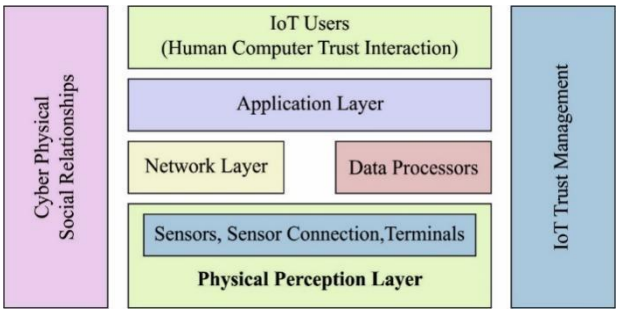


Figure 1. Trust Model of IoT System

Rapid increase in information and communications technologies (ICT), the healthcare sector is utilizing several applications, readily available technologies, infrastructure elements, and processes with organizations in other segments [3]. The networked or Internet-connected health devices could assist communications, electronic health records, efficient management of resources, and so on resulting in cost reductions (for example related to treatments and monitoring). A report predicted that networked technology might save more money for healthcare organizations in the future, viz., it could decrease the cost of hospital tools by 15 to 30% [4]. For example, the amount of data security breaches stated by healthcare providers increased by 60 % in 2014, which is approximately twice the rate created in other fields. As demonstrated by the current ransomware incident [5, 6], it is obvious that the healthcare industry isn't protected from cyber-attacks. It is because of widespread/intentional disruption (for example because of susceptibilities/flaws in operation, design, and implementation), privacy violations (for example compromise/leakage of sensitive medicinal records), and accidental failures. Though employing DL in network security was developed in recent times, the concept has attained considerable attention from the study [7, 8] because of the strong auto-learning capability of DL. Moreover, the development and improved availability of GPU processors considerably assist in speeding up matrices computation and huge scientific calculation, therefore it straightaway helps the possibility of DL-based methods. The DL for malicious traffic recognition is commonly classified into several kinds that are mainly dependent upon built-in network modules, for example, RNN unsupervised learning/ CNN, like AE. Reliability in IoT-enabled services rises as a critical concern since this service may be distorted by malicious users via changed/fake sensor data [9, 10].

This paper presents a new intelligent deep learning-based trust management with a decision-making tool (IDLTM-DMT) for healthcare big data environments using IoT. The proposed IDLTM-DMT model enables IoT devices to acquire health-related data. The IDLTM-DMT model involves a DL-based bidirectional long, short-term memory (BiLSTM) model for vulnerability finding and malicious traffic identification in the network. In addition, Hadoop MapReduce is used for handling big data. Moreover, a decision-making tool using a deep stacked autoencoder (DSAE) is used for the classification of diseases that exist in big data. For optimally modifying the hyperparameters engaged in the DSAE model, the sandpiper optimization (SPO) algorithm is employed thereby enhancing the detection performance. Neutrosophic Set Analysis is integrated to manage the indeterminacy and inconsistency of the data, enhancing the decision-making process. To examine the enhanced outcome of the IDLTM-DMT model, a series of simulations were performed on the EEG EyeState Dataset. The findings indicate that the proposed method achieves improved precision compared to existing methods, demonstrating the effectiveness of incorporating Neutrosophic Set Analysis [11] in IoT healthcare big data environments.

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

2. Related works

In [12], by Feng et al. a fog-based IoT healthcare architecture is proposed for minimizing the energy utilization of fog nodes. The study result reveals that the efficiency of the presented architecture is effective based on energy usage and network delay. Moreover, the researchers suggested and discussed vital services of big data framework that should be existing in fog devices for analyzing healthcare big data. Manogaran et al. [13] proposed a secured Industrial IoT framework for processing and storing scalable sensor big data for healthcare applications. Presented Meta Cloud-Redirection (MC-R) framework with sensor data knowledge scheme for collecting and storing the big data created from distinct sensor devices. In the presented scheme, sensor health devices are with the human body for collecting medical measures of the patients.

The major emphasis of this study is on securing the Authorization and Authentication of entire devices, Tracking and Identifying the devices placed in the scheme, tracking and locating mobile devices, novel things connection and placement to the present scheme [14], transmission among the devices and data transmission amongst remote healthcare schemes. Atitallah et al. [15] offer an analysis of the survey about the utilization of IoT and DL for developing smart cities. Later, they introduce the distinct computing frameworks utilized for IoT big data analysis that includes edge, cloud, and fog computing. Lastly, they summarize the present issues and challenges confronted in the growth of smart city service. Tuli et al. [16] propose a novel architecture named HealthFog to integrate ensemble DL in Edge computing devices and place it for real-time applications of automated heart disease analyses. Fog-enabled cloud architecture, FogBus is utilized for deploying and testing the efficiency of the presented module regarding network bandwidth, power consumption, jitter, latency, execution, and accuracy time. In [17] by Sharma et al., DeTrAs: DL-based Internet of Health architecture for the Aid of Alzheimer's persons are introduced. In [18] by Ahmad et al. an ANN, a framework of the DL method, is presented to effectively process smaller datasets. The involvement of this study is 2-fold. Initially, they presented a new method for building the ANN framework. This presented ANN framework contains subnets (sets of neurons) rather than layers, managed by a central technique.

In [19] by Mahmoud M et al. Neutrosophic Sets (NS) have been widely used to manage uncertainty in decision-making. Interval-valued Valued Neutrosophic Sets (IVNSs) are particularly effective in handling vague and ambiguous data, making them suitable for healthcare applications. Combining IVNSs with the TOPSIS method enhances the robustness of multi-criteria decision-making (MCDM). This study uses IVNSs and TOPSIS to evaluate mobile healthcare products, identify performance gaps, and propose improvements. The research contributes to the sustainable promotion of mobile healthcare by enhancing decision-making reliability and efficiency.

Zhou et al. [20] emphasize the DL improved HAR in the IoHT platform. A semi-supervised DL architecture is implemented and created for accurate HAR that efficiently utilizes and analyzes the weakly labeled sensor Training data for the classification learning module. To solve the challenges of ineffectively labeled instances, a smart auto-labeling system depending upon DQN is established with a recently implemented distance-based reward mechanism that can improve learning performance in IoT platforms. In [21] Kaur and Sharma have deliberated primarily, on numerous psychological and neurological disorders. The part of distinct computing methods in implementing distinct bio-medical applications was proposed. Additionally, the emphasis is on the problems and significant regions of innovations in implementing an intelligent and smart neurological disorder diagnosis scheme by IOT, big data, and emergent computing methods.

Varol et al. [22] introduced neutrosophic matrices and Neutrosophic Fuzzy Matrices (NFMs), which manage uncertainty, indeterminacy, and ambiguity in complex data. NFMs extend traditional matrices with neutrosophic logic, enhancing decision-making, image processing, AI applications, and Broumi discussed [31-32] the neutrosophic shortest route problem also. This research encourages the development of algorithms for specific decision-making challenges, emphasizing the significance of neutrosophic tools in advanced data analysis.

3. The Proposed Trust Management with Decision-Making Tool

The overall process involved in the proposed IDLTM-DMT model to accomplish trust management is given here. Initially, the BiLSTM model is applied to detect the vulnerabilities that exist in the IoT network and identify the manifestation of malicious traffic in the network. Neutrosophic set analysis is integrated to assess the trust levels of detected events. Each event is evaluated in terms of truthiness (T), indeterminacy (I), and falsity (F), allowing for a more nuanced determination of whether to block or allow traffic, thereby improving the model's ability to manage trust dynamically. Next, the DSAE model is employed to classify the existence of disease in the health-related data. Finally, the SPO algorithm is utilized for modifying the hyperparameters involved in the DSAE model and thereby enhance the detection performance. These processes are detailed in the succeeding subsections.

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

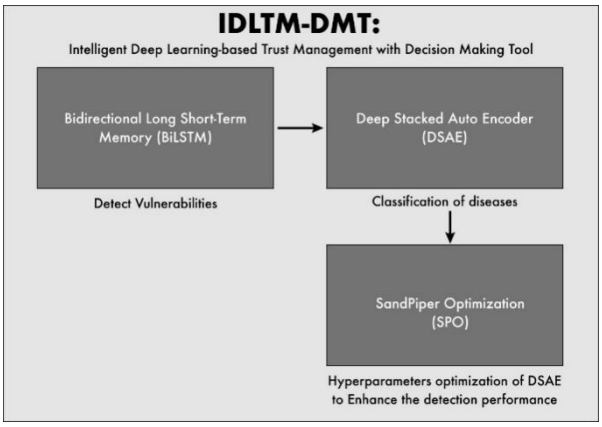


Figure 2. Proposed IDLTM-DMT Model

3.1. Trust based BiLSTM Model for Malicious Traffic Detection

The IDLTM-DMT model involves a DL-based BiLSTM model for vulnerability detection and thereby identifies the malicious traffic in the network. As healthcare ecosystems are more vulnerable than traditional networks, vulnerability detection techniques can be designed using the IDLTM-DMT technique uses neutrosophic set analysis to enhance this process, ensuring high trustworthiness and low false rates, which is critical to prevent unexpected accidents caused by falsely blocked devices.

Neutrosophic Set Analysis: Each detected anomaly is evaluated using neutrosophic sets to assess the trust level of the IoT devices. The trust level is quantified by:

- **Truthiness (T):** The degree of certainty that the detected behaviours is malicious.
- **Indeterminacy (I):** The uncertainty due to incomplete or ambiguous data.
- **Falsity (F):** The likelihood that the detected behaviours is benign.

This neutrosophic evaluation allows for more nuanced decisions regarding whether to block or allow traffic from the respective IoT devices.

In the healthcare environment, a low false rate is most needed as any falsely prevented devices result in an event of unexpected accident. For a trust-based IDS system, a BiLSTM model is applied to identify the malicious traffic and then the respective IoT devices get blocked. Then, the device can set up data flow to avoid that malicious location. The malicious data traffic is adequately conveyed by an abnormal nature. The abnormal utilization can be treated as a vulnerability. It is not easy to detect abnormal IoT devices. Therefore, the BiLSTM model is employed to detect malicious traffic in the network. In this way, this methodology can determine the trustworthy level of the IoT devices depending upon the long-term activity and offer high flexibility in the network.

An RNN is a different type of standard ANN that can model consecutive data with recurring links [23]. Fundamentally, it keeps a hidden state which is regarded as a memory of prior inputs. This is determined by every neuron that represent A function estimated from all prior data. The input units $\{\ldots, x_{t-1}, x_t, x_{t+1}, \ldots\}$ where $= (x_1, x_2, x_3, \ldots, x_N)$, are linked to the hidden units $h_t = (h_1, h_2, \cdots, h_M)$ in the hidden layer, through links determined with a weight matrix W_{IH}. All hidden entities are linked to the resulting one with recurring links as W_{HH}. Every hidden unit is equated as follows:

$$h_t = f_H(o_t) \tag{1}$$

Where:

$$o_t = W_{IH} + W_{HH} h_{t-1} + b_h \tag{2}$$

F_h denote nonlinear functions like sigmoid, tanh, ReLU and b_h indicates bias vectors. The hidden layer is linked with the resultant layer using weights W_{HO}. Finally, the outputs $y_t = (y_1, y_2, \ldots, y_P)$ are determined as follows:

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

$$y_t = f_O(W_{HO}h_t + b_o) \quad (3)$$

In a related way the hidden layer, f_O denotes activation function and b indicates bias vectors. Even though this module continues a memory of the prior state, actually it endures from the Vanishing gradient issue, making it impossible for long-term dependency. A distinct type of RNN named LSTM was introduced in 1997, which addresses this problem. The LSTM cell follows a more advanced method with the outline of a difficult cell that utilizes "forget" gate to select what to forget. Fig. 3 demonstrates the structure of LSTM.

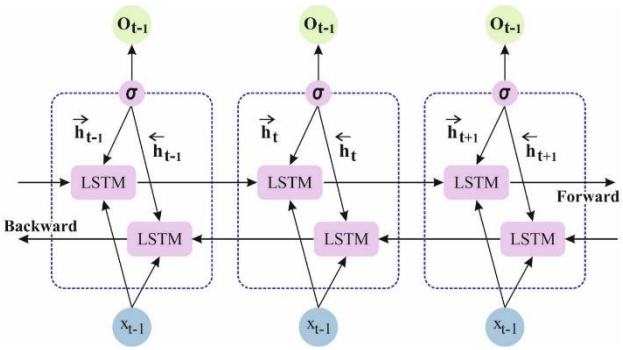


Figure 3. Structural design of LSTM

The state of the LSTM memory unit adapts the following numerical equation:

$$i_t = \sigma\,(W_{xi} + W_{hi}h_{t-1} + \mathrm{W}_{ci}c_{t-1} + b_i)$$

$$f_t = \sigma(W_{xf}x_t + W_{hf}h_{t-1} + \mathrm{W}_{cf}c_{t-1} + b_f)$$

$$c_t = f_t \otimes c_{t-1} + i_t \otimes tanh\,(W_{xc}x_t + W_{hc}h_{t-1} + b_c)$$

$$o_t = \Gamma(W_{xo}x_t + W_{ho}h_{t-1} + W_{co}c_t + b_o)$$

$$h_t = o_t \otimes tanh(c_t)$$

To clarify, the subscript for each matrix represents its function (Who denotes the hidden forget weight matrix). The variables f, o, i, and c correspond to the forget, output, input, and cell gate vectors, respectively. This setup allows the LSTM network to follow the structure of the previously discussed RNN framework, but with LSTM cells instead. An effective way to address this constraint is to use a precise replication of the LSTM network in reverse. By combining these techniques, a Bi-directional LSTM (BiLSTM) is formed, enabling the modeling of bidirectional dependencies.

3.2. Hadoop MapReduce

For managing Big Data, the Hadoop ecosystem and its components are extensively used [24]. Hadoop, an open-source framework, enables stakeholders to store and process Big Data across computer clusters with simplified programming models. This setup allows thousands of nodes on a single server to be configured, enhancing fault tolerance and scalability. The main three components of Hadoop are YARN, HDFS, and MapReduce. Within the MapReduce framework, the MRODC technique is employed to improve the efficiency and scalability of classifiers. The MRODC modules encompass the following factors:

- Calculate all sentence polarity scores using N-grams.
- Execute data classification based on the polarity scores.
- Evaluate new term frequencies and words from the classified data.

Various text mining methods are applied to pre-process the main data stored in HDFS. The Map function facilitates concurrent iteration, which is known as the Combiner function, the Reduce function, respectively.

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

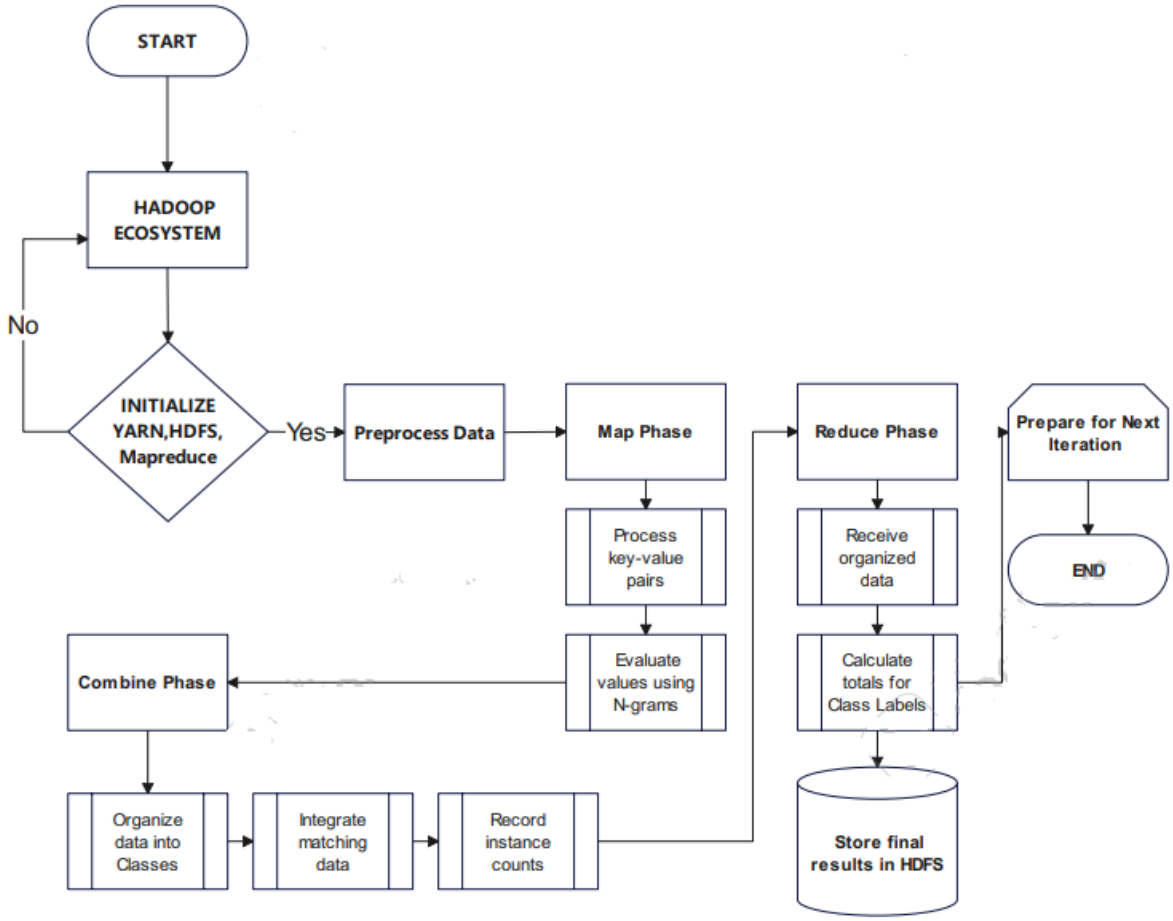


Figure 4. Demonstration of Map Reduce Process

Map phase

During the Map phase, each line is processed sequentially as pairs of key values, which serve as the input for the Map function. The function evaluates the values of all data objects based on the generated corpus and calculates scores using N-grams. The output from the Map function is then passed to the Combiner functions.

Combine phase

In the Combine phase, the Combiner function receives the data objects from the Map function and organizes them into equivalent classes. It then integrates all data with matching class values, records the instance counts, and transmits the results of each cluster to the Reducer functions.

Reduce phase

In the Reduce phase, the function receives all data from the Combiner function, organized into various classes. It then calculates the total amount of data for each class label and stores the final results in HDFS. The process prepares for the next iteration to begin.

3.3. DSAE based Classification Model

The AE is a type of unsupervised learning architecture that retains: output layer, input layer, and hidden layer. The process of an AE training contains decoder and encoder [25]. Assumed the unlabeled input dataset $\{x_n\}_{n=1}^{N}$, whereas $x_n \in R^{m\times 1}$, h_n denotes hidden encoder vectors evaluated from $\hat{x}_n$, and $\hat{x}$ represents decoding vectors of output layer. Henceforth the encoded procedure is given by:

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

$$h_n = f(W_1 x_n + b_1) \quad (4)$$

Whereas f denotes encoded function, W_1 indicates weight matrix of encoded, and b_1 represents bias vectors. The decoder procedure is determined by:

$$\hat{x}_n = g(W_2 h_n + b_2) \quad (5)$$

Where g indicates decoder function, where W_2 denotes the weight matrix of decoder, and b_2 denotes bias vector.

The variables set of the AE are enhanced for minimizing reconstruction error:

$$\phi(\theta) = \underset{\theta,\theta'}{\operatorname{argmin}} \frac{1}{n} \sum_{i=1}^{n} L(x^i, \hat{x}^i) \quad (6)$$

Where L refers the loss function

$L(x, \hat{x}) = \|x - \hat{x}\|^2$.

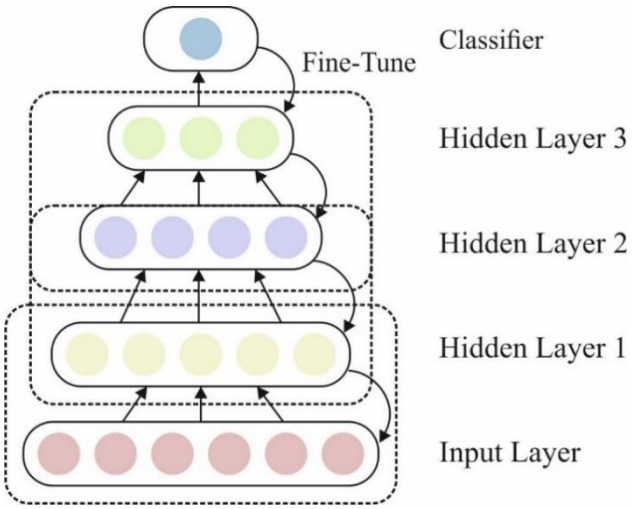


Figure 5. Structure of SAE

As shown in Figure 5, the architecture of a Stacked Autoencoder (SAE) involves stacking multiple AEs to form multiple hidden layers, using an unsupervised learning technique followed by fine-tuning with a supervised technique. The SAE-based technique consists of three stages:

1) Train the initial AE with input data to extract learned feature vectors.
2) Use feature vectors from the preceding layer as input for the subsequent layer, iterating this process until training concludes.
3) Finally, train the hidden layers using the backpropagation (BP) method to minimize cost function and adjust the weights, with the labelled data fixed to achieve fine-tuning.

3.4. Hyperparameter Optimization using SPO Algorithm

To optimally adjust the hyperparameters of the DSAE model, the Sandpiper Optimization (SPO) algorithm is employed, enhancing detection performance. Sandpipers are seabirds found globally, known for their colony living and their behaviors in hunting and migration. Migration is a seasonal movement where sandpipers travel to locate abundant food sources for energy. During migration, they exhibit a distinctive spiral motion when attacking, which can be related to the optimization objective function. This study focuses on two natural behaviors of sandpipers:

Migration behavior: This involves the movement patterns of sandpipers during migration. A sandpiper must satisfy three conditions:

Collision avoidance: Variables C_A are used to calculate new positions for search agents, ensuring they avoid collisions with neighboring sandpipers.

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

$$\overrightarrow{C_{sp}} = C_A \times \overrightarrow{P_{sp}}(z) \quad (7)$$

Whereas $\overrightarrow{C_{sp}}$ denotes placement of a search agent to prevent collision with another search agents, $\overrightarrow{P_{s\rho}}$ determines present search agent location, z represents existing iteration, and C_A indicates movement of search agent in a search space.

$$C_A = C_f - \left(z \times \left(C_f / \text{Max}_{iterations}\right)\right)$$

Where,

$$z = 0, 1, 2, \ldots, \text{Max}_{iterations} \quad (8)$$

Let C_f represents control frequency for adjusting the parameter C_A that reduced linearly from C_f to 0. When variable C_f is fixed to two, the variable C_A is always decreased from two to zero. The value of C_f is fixed to two in this study [26].

Converge in the direction of best neighbors: After collision avoidance, search agent converges (viz movement) to the direction of an optimum neighbor.

$$\overrightarrow{M_{sp}} = C_B \times \left(\overrightarrow{P_{bst}}(z) - \overrightarrow{P_{sp}}(z)\right) \quad (9)$$

Whereas $\overrightarrow{M_{sp}}$ denotes location of search agent, $\overrightarrow{P_{sp}}$ indicates optimum fittest search agent $\overrightarrow{P_{bst}}$ (viz., that fitness value is lesser). C_B represents arbitrary parameter that is in charge of an optimum exploration. The C_B is calculated by:

$$C_B = 0.5 \times R_{and} \quad (10)$$

whereas R_{and} denotes arbitrary amount lies in the range of zero and one.

Updated with respect to best search agent: Finally, the search agent/sandpiper could enhance its location equivalent to an optimum search agent.

$$\overrightarrow{D_{sp}} = \overrightarrow{C_{sp}} + \overrightarrow{M_{sp}} \quad (11)$$

where $\overrightarrow{D_{sp}}$ measures the gap between search agents and the most fit search agents.

During migration, sandpipers can continuously adjust their attack angle and speed. They use their wings to increase their altitude and create a spiral pattern when attacking prey in the air. This three-dimensional behavior can be described as follows:

$$x^f = R_{adius} \times sin(i) \quad (12)$$

$$y^f = R_{adius} \times cos(i) \quad (13)$$

$$z^f = R_{adius} \times i \quad (14)$$

$$r = u \times e^{kv} \quad (15)$$

Let R_{adius} denotes radius of each turn in the spiral, where i denotes the parameter lies from range of $[0 \leq k \leq 2\text{A}]$. u and v represent constant to determine spiral form, and e denotes base of the natural logarithm. Noted that in this study, they consider the value of constant u and v as one.

4. Performance Validation

This section evaluates the performance of the proposed IDLTM-DMT model, enhanced with neutrosophic set analysis, against existing techniques. The Mirai-RGU dataset from Robert Gordon University, which includes Mirai-based DDoS traffic, is used. This dataset comprises various types of Mirai botnet traffic such as Scan, Infect, Control, and Attack, along with normal IoT IP Camera traffic. It features ten types of malicious traffic, including VSE flood, TCP SYN flood, UDP flood, Mirai traffic, DNS flood, GREETH flood, TCP ACK flood, HTTP flood,

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

GREIP flood, and UDPPLAIN flood. The dataset attributes include Length, Time, Destination, Source, Protocol, and overall Payload data. The model's parameter settings are as follows: a learning rate of 0.01, a dropout rate of 0.5, 64 neurons in the LSTM hidden layer, and a batch size of 64. Figure 5 illustrate the detection performance of the proposed model on the Mirai-RGU dataset across various metrics [27]. The results indicate that the proposed model, with neutrosophic set analysis, achieves superior detection performance under different training set ratios.

Accuracy - This crucial parameter measures the overall correctness of the model; higher accuracy indicates a more secure model.

$$\frac{\text{True Positive} + \text{True Negative}}{\text{True Positive} + \text{False Positive} + \text{False Negative} + \text{True Negative}}$$

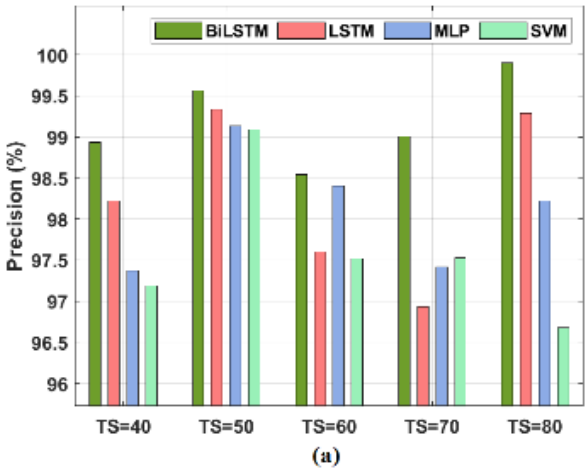
Precision - This metric represents the ratio of true positive predictions to the total predicted positive observations.

$$\frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

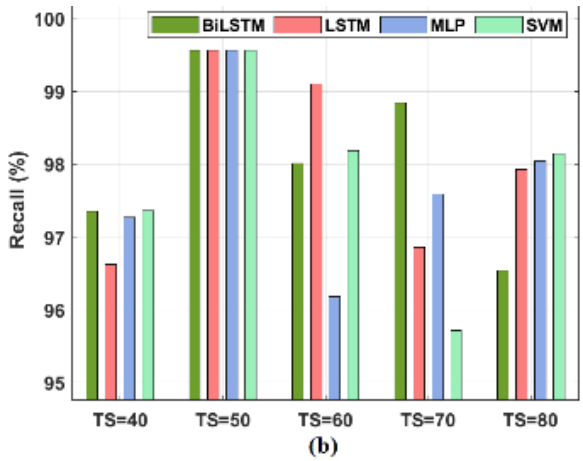
Recall (Sensitivity) - This metric denotes the ratio of accurately predicted positive observations to all actual positive observations.

$$\frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}}$$

On examining the results in terms of precision, it is evident that the SVM model has reached the lowest performance with an average precision of 97.60%. Eventually, the LSTM and MLP models have exhibited moderately closer outcomes with an average precision of 98.22% and 97.37% respectively. However, the BiLSTM model, enhanced with neutrosophic set analysis, demonstrates superior performance with a maximum average precision of 99.19%.



(a)



(b)

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

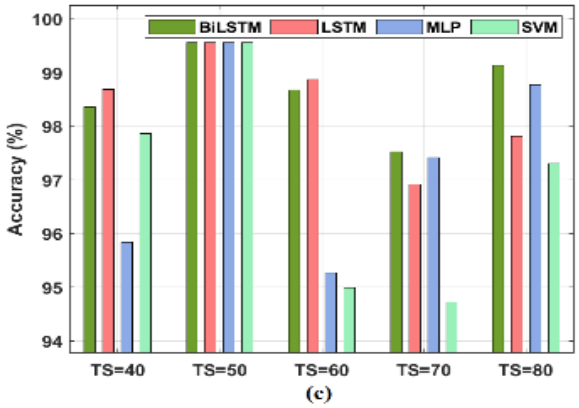


Figure 6. Result analysis of BilSTM Model on Mirai-RGU Dataset

Finally, on analyzing the outcomes with respect to recall, it's stated that the SVM method has attained the least performance with the average recall of 97.79%. Likewise, the LSTM and MLP approaches have showcased moderately closer result with an average recall of 98.01% and 97.73% respectively. The BiLSTM method, with neutrosophic set analysis, showcases better performance with a maximal average recall of 98.06%. Finally, on determining the results in terms of accuracy, it is observed that the SVM technique has reached a poor performance with an average accuracy of 96.89%. At the same time, the LSTM and MLP manners have demonstrated moderately closer outcomes with the average accuracy of 97.37% and 98.37% respectively. The BiLSTM algorithm, with neutrosophic set analysis, achieves higher performance with a maximal average accuracy of 98.65%.

On the other hand, the classification performance of the presented model is tested utilizing the EEG Eye Sate dataset [28] which encompasses 14980 samples with 15 attributes. From the existing samples, 8257 samples fall into class 1 and the rest of the 6723 samples comes under class 2. Every sample data has 14 EEG attributes with an eye-state class (0-open and 1- closed). Table 2 and Figure. 6 shows the classification results analysis of the presented IDLTM-DMT model with the DSAE technique. The resultant values demonstrated that the DSAE model has offered a precision of 91.44%, recall of 90.10%, F-measure of 91.95%, and accuracy of 91.03%. The proposed IDLTM-DMT method, enhanced with neutrosophic set analysis, achieves higher precision 96.90%, recall 97.34%, F-measure 97.19%, and accuracy 97.28%.

Table 1: Performance Analysis of Proposed Methods for EEG EyeState Dataset

Methods	Precision	Recall	F-Measure	Accuracy
IDLTM-DMT	96.90	97.34	97.19	97.28
DSAE	91.44	90.10	91.95	91.03

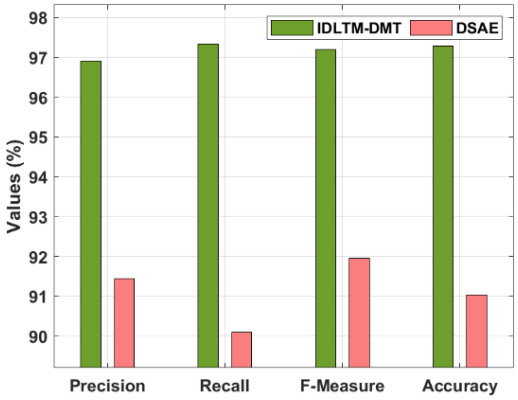


Figure 6. Result analysis of IDLTM-DMT model with different measures

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

A comprehensive comparative study of the IDLTM-DMT model alongside other existing techniques takes place on EEG Eye State Dataset is given in Table 1 [29,30]. From the obtained values, it is apparent that the linear SVM and HMM models have offered lowest outcome with the accuracy of 0.5512 and 0.5512. Besides, the RNN, GRU, and LSTM approaches have accomplished slightly increased performance with the accuracy of 0.7894, 0.8065, and 0.8178 respectively. Moreover, the SA-LSTM, DE-RNN, RS-LSTM, DE-GRU, and DE-LSTM models have demonstrated moderately closer performance. Though the DSAE model has showcased near optimal performance with the accuracy of 0.9103, the proposed IDLTM-DMT technique, with neutrosophic set analysis, results in a maximal accuracy of 0.9728.

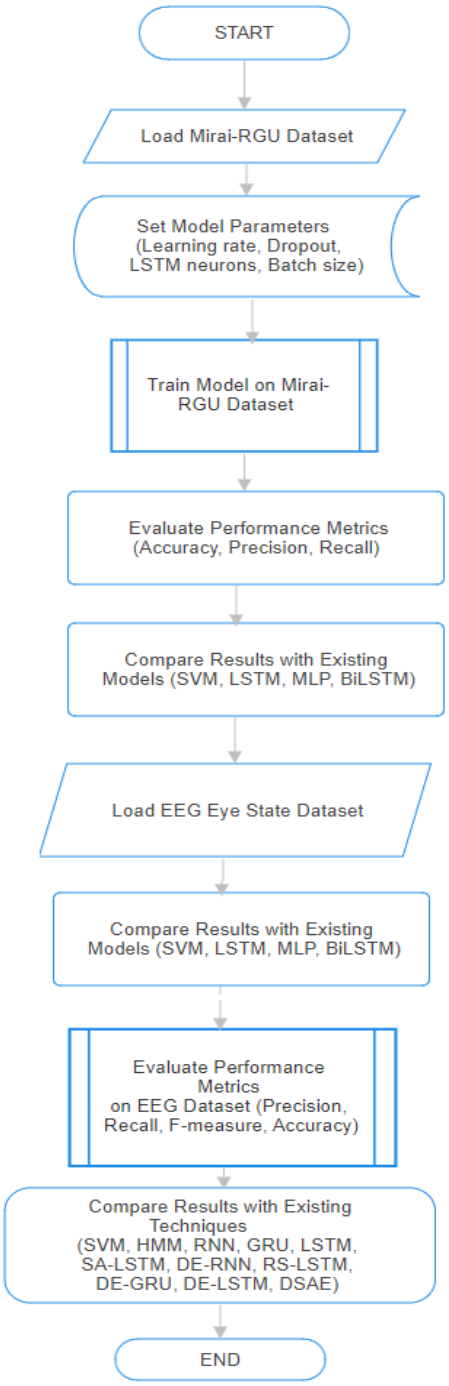


Figure 7. Flowchart of Result Performance Validation Process

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

Table 2: Comparison of Proposed IDLTM-DMT with Neutrosophic Set Analysis on EEG Eye State Dataset with Other Techniques

Methods	**Accuracy**
IDLTM-DMT with Neutrosophic Set Analysis	0.9728
DSAE	0.9103
DE-LSTM	0.8852
DE-GRU	0.8714
DE-RNN	0.8523
RS-LSTM	0.8711
SA-LSTM	0.8449
GRU	0.8065
RNN	0.7894
LSTM	0.8178
Linear SVM	0.5512
HMM	0.5512

The above-cited tables and figures ensure that the IDLTM-DMT method, with neutrosophic set analysis, is an effective tool for achieving security in IoT and big data-based healthcare environments. It can be employed as a reliable malicious traffic detection and disease diagnostic model in the healthcare sector, offering superior performance metrics compared to existing techniques.

5. Conclusion

This paper has proposed a novel IDLTM-DMT model to enhance security and decision-making processes in the healthcare sector. The IDLTM-DMT model incorporates Hadoop MapReduce for managing big data, BiLSTM for malicious traffic detection, DSAE for disease classification, and SPO for hyperparameter tuning. The BiLSTM model effectively detects network vulnerabilities and identifies malicious traffic, while the DSAE model classifies diseases within the healthcare data, optimized by the SPO algorithm. Additionally, Neutrosophic Set Analysis is integrated to handle data indeterminacy and inconsistency, further improving decision-making accuracy. Extensive simulations conducted on the EEG EyeState Dataset reveal that the proposed method achieves improved precision equated to existing methods, demonstrating the effectiveness of incorporating Neutrosophic Set Analysis in IoT healthcare big data environments. Future work may focus on incorporating lightweight cryptographic techniques to enhance security and trust management.

Funding: "This research received no external funding"

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

References

[1] R. Annamalai, "Efficient Solution to the Waste Management Process Using IOT for Smart Trash Can" , *Journal of Emerging Technologies and Innovative Research*, Volume 5, Issue 6, June 2018.

[2] W. Shi, S. Liu, J. Zhang, and H. Wang, "Deep learning-based image classification for UAV applications: A review of methods, datasets, and challenges," *Remote Sensing*, vol. 12, no. 14, pp. 2334-2348, 2020, DOI: 10.3390/rs12142334.

[3] Meng, W., Choo, K.K.R., Furnell, S., Vasilakos, A.V. and Probst, C.W., "Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks", *IEEE Transactions on Network and Service Management*, *15*(2), pp.761-773. 2018.

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

[4] Divyabharathi. S, "Large scale optimization to minimize network traffic using MapReduce in big data applications", *International Conference on Computation of Power, Energy Information and Communication (ICCPEIC)*, pp. 193-199, April 2016.

[5] B. Chappell and M. Penman., "Ransomware Attacks Ravage Computer Networks in Dozens of Countries.", Nov. 15, 2017.

[6] Lakshmanaprabu, S.K., Shankar, K., Rani, S.S., Abdulhay, E., Arunkumar, N., Ramirez, G. and Uthayakumar, J., "An effect of big data technology with ant colony optimization-based routing in vehicular ad hoc networks: Towards smart cities", *Journal of cleaner production*, 217, pp.584-593. 2019.

[7] Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D. N, "BaIoT-Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders.", *IEEE Pervasive Comput. 2018*, 17, 11–22, 2019.

[8] S.Neelakandan, S.Muthukumaran, "Transformation-based Optimizations Framework (ToF) for Workflows and its Security issues in the Cloud Computing.", International *Journal of Engineering and Computer Science*, 4(08).

[9] Shayesteh, B., Hakami, V. and Akbari, A., "A trust management scheme for IoT-enabled environmental health/accessibility monitoring services". *International Journal of Information Security*", 19(1), pp.93-110, 2020.

[10] Berlin, M.A., Tripathi, S. et al. "IoT-based traffic prediction and traffic signal control system for smart city", soft *Computing*, 2021.

[11] Manshath, A., E. Kungumaraj, E. Lathanayagam, MC Joe Anand, Nivetha Martin, Elangovan Muniyandy, and S. Indrakumar. "Neutrosophic Integrals by Reduction Formula and Partial Fraction Methods for Indefinite Integrals." *Journal of International Journal of Neutrosophic Science*, vol. 23, no. 1, pp. 08-16, 2024

[12] Z. Li, X. Zhang, H. Wang, and Y. Zhou, "AI-driven optimization in healthcare decision-making: Applications in farmland fertility and disease detection," *Expert Systems with Applications*, vol. 179, pp. 115009, 2021, DOI: 10.1016/j.eswa.2021.115009.

[13] Manogaran G., Thota C., Lopez D., Sundarasekar R., "Big Data Security Intelligence for Healthcare Industry 4.0", Thames L., Schaefer D. (eds), Cybersecurity for Industry 4.0. Springer Series in Advanced Manufacturing. Springer, Cham., 2017

[14] Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R. and Priyan, M.K., "Centralized fog computing security platform for IoT and cloud in the healthcare system", *In Fog computing: Breakthroughs in research and practice*, pp. 365-378. IGI Global. 2018.

[15] Atitallah, S.B., Driss, M., Boulila, W. and Ghézala, H.B., "Leveraging Deep Learning and IoT big data analytics to support the smart Cities development: Review and future directions.", *Computer Science Review*, 38, p.100303, 2020.

[16] Tuli, S., Basumatary, N., Gill, S.S., Kahani, M., Arya, R.C., Wander, G.S. and Buyya, R., " HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments", *Future Generation Computer Systems*, 104, pp.187-200, 2020.

[17] Sharma, S., Dudeja, R.K., Aujla, G.S. et al., "DeTrAs: deep learning-based healthcare framework for IoT-based assistance of Alzheimer patients. Neural Comput & Applic", 2020.

[18] Ahmad U. et al. "A Novel Deep Learning Model to Secure Internet of Things in Healthcare. In: Maleh Y., Shojafar M., Alazab M., Baddi Y., "Machine Intelligence and Big Data Analytics for Cybersecurity Applications. Studies in Computational Intelligence", vol 919. Springer, Cham, 2021.

[19] Mahmoud M. Ismail "Interval Valued Neutrosophic Sets and Multi-Criteria Decision Making for Sustainable Mobile Healthcare Promotion," *Journal of Financial Technology and Innovation*, vol. 1, no. 1, pp. 08-15, 2022.

[20] Zhou, X., Liang, W., Kevin, I., Wang, K., Wang, H., Yang, L.T. and Jin, Q., "Deep-learning-enhanced human activity recognition for Internet of healthcare things", *IEEE Internet of Things Journal*, 7(7), pp.6429-6438, 2020.

[21] Kaur, P. and Sharma, M., "A Smart and Promising Neurological Disorder Diagnostic System: An Amalgamation of Big Data, IoT, and Emerging Computing Techniques. Intelligent Data Analysis: From Data Gathering to Data Comprehension", pp.241-264, 2020.

[22] Varol, S. R., Şahin, R., and Başağa, H. "Neutrosophic Matrices and Their Applications in Handling Indeterminacy." *Journal of Neutrosophic Research* 5, no. 1 (2017): 25-34.

[23] Pogiatzis, A. and Samakovitis, G., "Using BiLSTM Networks for Context-Aware Deep Sensitivity Labelling on Conversational Data", . *Applied Sciences*, *10*(24), p.8924, 2020.

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024

[24] Selvi, R.T. and Muthulakshmi, I., "Modelling the map-reduce based optimal gradient boosted tree classification algorithm for diabetes mellitus diagnosis system", *Journal of Ambient Intelligence and Humanized Computing*, 12(2), pp.1717-1730, 2021.

[25] Liu, G., Bao, H. and Han, B., "A stacked autoencoder-based deep neural network for achieving gearbox fault diagnosis", *Mathematical Problems in Engineering*, 2018.

[26] Kaur, A., Jain, S. and Goel, S., "Sandpiper optimization algorithm: a novel approach for solving real-life engineering problems", *Applied Intelligence, 50*(2), pp.582-619, 2020.

[27] Hwang, R.H., Peng, M.C., Nguyen, V.L. and Chang, Y.L., "An LSTM-based deep learning approach for classifying malicious traffic at the packet level", *Applied Sciences*, *9*(16), p.3414, 2019.

[28] S. Nithyanantham, V. Nishanth, A. Prakash, and D. Kaviyarrasu, "Smart city ambulance for tracking shortest path using global position system.", *International Journal of Engineering & Technology* 7, no. 1.3, 2017

[29] https://archive.ics.uci.edu/ml/datasets/EEG+Eye+State

[30] Prakash Mohan, Manikandan Sundaram, "An Analysis of Air Compressor Fault Diagnosis using Machine Learning Technique", *Journal of Mechanics of Continua and Mathematical Sciences*. Vol.-14, No.-6, pp 13-27 ISSN: 0973-8975, November - December 2019.

[31] Broumi, S., Mohanaselvi, S., Witczak, T., Talea, M., Bakali, A., & Smarandache, F. (2023). Complex fermatean neutrosophic graph and application to decision making. Decision Making: Applications in Management and Engineering, 6(1), 474-501.

[32] Broumi, S., Raut, P. K., & Behera, S. P. (2023). Solving shortest path problems using an ant colony algorithm with triangular neutrosophic arc weights. International Journal of Neutrosophic Science, 20(4), 128-28.

DOI: https://doi.org/10.54216/IJNS.240430
Received: November 24, 2023 Revised: February 09, 2024 Accepted: May 22, 2024