Anomaly-Based Intrusion Detection System in WSN using DNN Algorithm

Belal Al-Fuhaidi, Zainab Farae, Wedad Al-Sorori,
Naseebah Maqtary, Yahya Al-Ashmoery, Farouk Al-Fuhaidy and
Sadiq Al-Taweel

June 27, 2025

Anomaly-Based Intrusion Detection System in WSN using DNN Algorithm

1st Belal Al-Fuhaidi[C]
Faculty of Computing and IT,
University of Science and Technology,
Sana'a, Yemen
belalarh@gmail.com, belalarh@ust.edu.ye

2nd Zainab Farae
Faculty of Computing and IT,
University of Science and Technology,
Sana'a, Yemen
zainabfarae@gmail.com

3rd Wedad Al-Sorori
Faculty of Computing and IT,
University of Science and Technology,
Sana'a, Yemen
w.alsorori@gmail.com

4th Naseebah Maqtary
Faculty of Computing and IT,
University of Science and Technology,
Sana'a, Yemen
n.almaqtary@gmail.com

5th Yahya Al-Ashmoery
Department of IT, Al-Razi University
Dept. Mathematics & Computer
Faculty of Science, Sana'a University
Sana'a,Yemen
Yah.AlAshmoery@su.edu.ye

6th Farouk Al-Fuhaidy
Department of Electrical Engineering,
Faculty of Engineering,
Ibb University, Ibb, Yemen,
farouqakh@gmail.com

7th Sadik Al-Taweel
Faculty of Computing and IT,
University of Science and Technology,
Sana'a, Yemen
altaweel.sadik@gmail.com

***Abstract*— Intrusion detection systems (IDSs) are a necessary principle in WSN security, which can successfully prevent various hackers' and intruders' attempts to hack the network. In this research, we address the problem of achieving high accuracy in detecting intrusions in WSNs due to specific characteristics of WSN data, including the appropriate dataset, the drawbacks of feature selection, and choosing the proper algorithms for the classification process. In this paper, we proposed the anomaly-based IDS model using the DNN algorithm and mutual information (MI) technology to select features. The proposed model has been implemented using the Python language used in the Anaconda platform and relying on the standard NSL-KDD dataset. The experimental results showed the capability of the proposed model to achieve high-performance accuracy in intrusion detection using the DNN algorithm compared to the state-of-the-art. The proposed model outperforms other previous relevant works by 3.65% enhancement in terms of accuracy.**

Keywords—IDS, Deep Learning, WSN, DNN, mutual information (MI) technology.

I. Introduction

WSN refers to a wireless network with several sensors. Nodes that are intensively placed either. Within or extremely close to the physical phenomenon. [1] to describe, monitor, and respond to an occurrence or a phenomenon [2]. WSNs confront several security difficulties because of the nature of the wireless communication medium, such as espionage, spoofing, distributed DoS, and other attacks. IDSs are a necessary principle in WSN security, which can prevent hackers' and intruders' attempts to hack the network. James Anderson was the one who first presented the concept of IDS in 1980. Now, IDS is a crucial component and a key responsibility of network administrators [3] IDS is the system for analyzing and monitoring network traffic and system activities to detect weaknesses and attacks and alert administrators if anything is detected. IDS types can be classified into host-based IDS (HIDS) and network-based IDS (NIDS). The HIDS aims to monitor internal computer activity, the attacks on a specific host, security of system logs, system files, and registry keys is guaranteed [4]. NIDS is a system to monitor a network's traffic records in real-time and dynamically to find any possible network intrusions by using the appropriate detection algorithms [5]. Anomaly-based IDSs, signature-based IDSs, and hybrid-based IDS are significant kinds of NIDS. Where Anomaly-based IDSs utilize classification algorithms, evaluate network activity, and classify it as normal or an attack. The vast majority of the time, IDSs use threshold limits to detect intrusions. In other words, any behavior below a specific threshold is considered normal, while any event above that barrier is considered an intrusion. The capacity of anomaly-based IDSs to detect new and unknown assaults is its primary advantage [6].

Machine learning (ML) and deep learning (DL) algorithms are typically used to create precise models primarily intended for prediction, classification, and clustering tasks. DL algorithms are a subset of ML algorithms that can also remove a few of the constraints of ML algorithms. DL algorithms are used in a variety of applications. DL is primarily concerned with both the detection of anomalies and the more precise analysis of network data [7].

Many studies based on DL have been published on IDSs, IDSs in networks, and IDSs in WSNs. We review studies of IDSs that have been designed and can be used with different types of wired and wireless networks.

Authors in [8] designed an IDS using back propagation neural networks (BPN) and a SOM and compared their performance. The KDD99 standard dataset was used to measure the designed system performance; The result was that the performance of SOM was better than BP. [9] proposed an IDS that combined the SVM algorithm and the Bee Colony (BC) algorithm, named CSVBC. Then, CSVAC was applied, which combined the Ant Colony (AC) and SVM algorithms. The KDD99 dataset was used to implement and measure the proposed system. The results demonstrated that combining the two methods, SVM and BC produced better classification accuracy than either method alone. Furthermore, when comparing CSVBC and CSVAC, the proposed system achieved the highest accuracy (88.56%).

979-8-3315-3355-7/24/$31.00 ©2024 IEEE

Researchers in [10] proposed an intrusion detection model using Artificial Neural Networks (ANN) for classification and the correlation-based feature selection (CFS) technique for feature selection. The model's performance was compared with the performance of a group of ML algorithms, and the model's performance before and after feature selection was compared. To implement and measure the performance of the proposed system, it relied on the standard datasets NSL-KDD and UNSW-NB. The result was that the model that used neural networks and feature selection achieved high performance in intrusion detection compared to ML algorithms' performance. The accuracy achieved with the UNSW-NB dataset was 96.44%, and with the NSL-KDD dataset, 97.49%. A study in [11] proposed the model for intrusion detection using an autoencoder model (AE) and loss functions with mean absolute error (MAE), which provided high model accuracy. To implement and measure the performance of a proposed system, it relied on an NSL-KDD standard dataset. The model achieved high performance in detecting intrusion, with an accuracy of 90.61%. Authors in [7] proposed the model for intrusion detection using the DNN algorithm and XGBoost technology for selecting features. To implement and measure the performance of a proposed system, it relied on an NSL-KDD standard dataset. The result was that a proposed model achieved higher accuracy than the performance of other ML algorithms, such as Naive Bayes, LR, and SVM, which achieved a 97% accuracy rate. [12] proposed IDS using DL and a sparse auto-encoder to learn features and a logistic classifier for classification. The NSL-KDD standard dataset was used to implement and measure system performance. The results indicate that the proposed system had an accuracy of 87.2% in detecting intrusions into the network. Authors in [13] suggested an IDS that employed the autoencoders' method. An NSL-KDD standard dataset was used to implement and assess the performance of a suggested system. The result was that a suggested system obtained an accuracy of 91.70%, compared to the previous study that used cluster analysis algorithms and obtained an accuracy of 80%. [14] published a study that reviewed two IDSs using fuzzy logic and an artificial neural network assembled into a system called (FC-ANN), directly comparing several ML-NIDS techniques. A standard dataset KDD99 was used to implement and evaluate a proposed system's performance. The result was that an FC-ANN-based approach increased the detection rate compared with the several ML-NIDS approaches, resulting in a detection of 80.70 %.

Authors in [15] proposed an IDS named PSO-FLN in which a PSO-based fast learning network (FLN) was used to achieve high performance. The suggested system was compared to a group of algorithms. A standard dataset, KDD99, was utilized to implement and assess the effectiveness of a suggested system. The results demonstrated that this test model outperformed other models in learning accuracy, such as ELM and FLNs, where it achieved a detection accuracy of 98 percent. [16] developed an IDS by applying a clustering approach in an optimization algorithm: a random subspace with an extreme learning machine (ELM) as the base class. The Bat Algorithm (BA)--based ensemble pruning strategy enhanced the ensemble model and optimized the sorted subset. A fitness function that depends on an ensemble's accuracy and variety is determined in the BA. The following standard datasets were utilized to apply and measure the performance of a proposed system: KDD 1999, NSL-KDD, and Kyoto. The result was that the random subspace-based group method achieved a high detection rate when using ELM individually. When using all sub-categories in the group, the pruning framework achieved better performance in the intrusion detection system, as it achieved 98.94%. A study in [17] introduced a study on how well IDSs perform in computer networks using hybrid ML approaches. The following techniques employed K-means for unsupervised learning and neural networks (NN) and SVM with radial kernel algorithms for supervised learning. As feature selection methods, PCA and Gradual Feature Reduction (GFR) are studied. The NSL-KDD standard dataset was utilized to put the suggested system into practice and assess its performance. The outcomes demonstrated that the NN model using GFR2 performed better, achieving an accuracy of 88.68% in identifying network intrusions.

We review studies of IDS in WSNs designed to monitor and detect any unexpected activity. Authors in [18] proposed an IDS using a DNN and a cross-correlation approach to select features. To implement and measure the performance of a proposed system, it relied on the standard dataset NSL-KDD. The result was that the proposed IDS achieved high performance in intrusion detection, where it achieved an accuracy of 95.53 %. [19] proposed IDS using a multi-kernel extreme learning machine (MK-ELM) for classification; the model performance was compared with SVM and bare ELM. To implement and assess the effectiveness of a suggested system, a standard dataset UNSW-NB 15 was used. The result was that the model achieved better performance detecting intrusions than other algorithms, such as SVM and ELM, as its accuracy was 98.3%. [20] introduced an IDS, Restricted Boltzmann Clustered (RBC); the system performance was compared to that of an adaptively supervised and clustered hybrid (ASCH). To implement and assess the effectiveness of a suggested system, it relied on a dataset KDD'99. The result was that the proposed IDS achieved high performance in intrusion detection. The accuracy achieved was 99.91%.

The security of WSNs has recently emerged as a critical source of concern, and the increase in attacks and threats against networks has become a severe problem that threatens network security. To resolve it, it is essential to analyze network traffic and classify it as normal or an attack, "a binary classification problem [21, 7]. Moreover, network traffic can also be considered a "multi-class classification problem" in which it is classified as a normal or a specific attack using IDS. Passive and active defense are the two main categories of Wireless Sensor Network (WSN) security studies. There are far too few studies on active defense for WSNs compared to the advancement of passive defense research for WSNs. On the other hand, passive defense is a measure implemented in reaction to the features of an assault after the attack has occurred, which is insufficient for security in WSNs. As a result, it is critical to investigate active defense systems that can analyze network traffic and detect malicious intrusions before they cause an attack. IDS will have a significant impact on ensuring the security of WSNs because it is an active defense technique [22].

However, these IDSs suffer from several drawbacks, which affect their effectiveness and flexibility in accuracy, so they must be overcome to improve their performance of IDS. These drawbacks include difficulty in determining the appropriate dataset [14], choosing the appropriate method for data normalization [3] choosing the appropriate new algorithms for the classification process [23]; Moreover, using all the features in datasets, some of which may not be important and do not affect the classification process [24].

In summary, from the previous reviews, The increase in attacks and threats against wireless networks and wireless sensor networks has become a serious problem to be solved. We must analyze the network traffic and classify it into normal or abnormal attacks (binary classification). Abnormal network traffic can also be classified into multiple types of attacks. "Multi-class classification". Intrusion detection systems play an important role in securing networks and wireless sensor networks, as they constitute an active defense strategy. However, these intrusion detection systems suffer from several drawbacks that affect their effectiveness and flexibility in accuracy, so they must overcome them to improve their performance as intrusion detection systems. These drawbacks include difficulties in identifying the appropriate dataset. Choosing the proper method for normalizing the data, choosing new algorithms suitable for the classification process, and using all the features in the dataset, some of which may be unimportant and do not affect the classification process. The paper proposes a deep learning (DL) model that analyzes and classifies network traffic as normal and attacks, as well as normal or specific attacks, and attempts to overcome these shortcomings in intrusion detection systems to provide high performance and accuracy in intrusion detection. This research proposes a model for anomaly-IDS in WSNs using the DNN algorithm. The proposed model is an effort to analyze network traffic and detect abnormal events. Moreover, it applies feature selection using the filter technique "MI", to conduct a comparative study of the proposed model with the state-of-the-art.

The rest of the paper is organized as follows. Section II outlines the proposed model using the DL algorithm. Section III presents the DNN classification algorithm briefly. Section IV explains the experimental setup and the comparison results of the proposed model against existing methods. Section V concludes the paper and lists future works.

II. THE PROPOSED MODEL USING DL ALGORITHM

In wireless sensor networks (WSN), different types of traffic data are transmitted through wireless sensor nodes to the sink. Before that, an intrusion detection system monitors and analyzes the traffic data; if an intrusion occurs, an alert is sent to the administrators to take proper action to prevent the intrusion. The IDS is inducted between the firewall and the sink, as shown in Fig. 1.

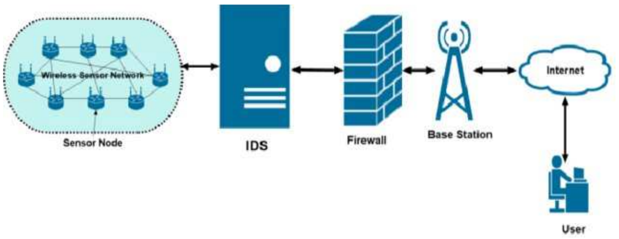

Fig. 1. IDS in wireless sensor networks

Below is a brief description of the steps used in this research for the proposed model based on deep learning (DL) algorithms as shown in Fig. 2.

1. Load NSL-KDD dataset.
2. Pre-processing for dataset.
   - Implement label encoding to convert non-digital features into digital features.
   - Implement feature scaling 'normalization ' conducted to normalize the data within a specific range.
3. Implement technique ' MI to feature selection.
4. Split the dataset into two parts: training and testing.
5. Training and Testing the DL Algorithm on the pre-processed dataset
6. Performance evaluation.
7. Results analysis
8. Comparison of results

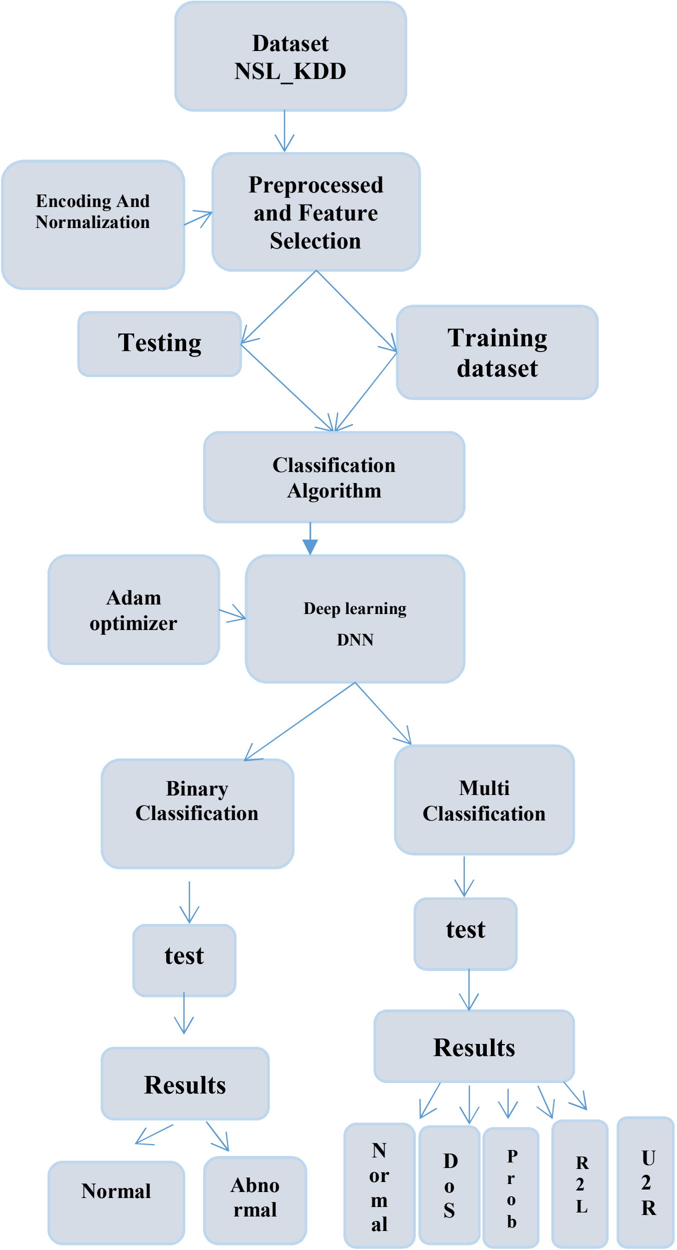

Fig. 2. The diagram of the proposed model with DL

In the research, a classifier algorithm is used in the IDS model. These classifiers are typically based on the DL algorithm, which is within supervised learning. These algorithms are specifically designed as classifiers, which are used to determine if network access has been normal or attacks. This algorithm is introduced in more detail in the following section.

A. NSL-KDD Dataset

Creating a large amount of network traffic data for testing a proposed model is complex. Due to that, this study has used the NSL-KDD evaluation dataset as a reference point for analysing the performance of the proposed model. This dataset is an enhanced version of KDD99. It is a sample dataset that is most commonly used for evaluating network traffic analyses for intrusion detection, and it is still widely regarded as one of the most comprehensive, trustworthy, and reliable public datasets in the field of an IDS [25]. From a review of the literature, it was found that 41% of the researches used NSL-KDD for testing and validation purposes; This was also used by 36% (Ahmad et al., 2021). It has 148517 connection records. Each record has 41 different features shown as the following [25]:

Feature Name: Duration, Protocol_type, Service, Flag, Src_bytes, Dst_bytes, Land, Wrong_fragment, Urgent, Hot, Num_failed _logins, Logged_in, Num_compromised, Root_shell, Num_file_creations. Su_attempted, Num_root, Num_shells, Num_access_files, Num_outbound_cmds, Is_hot_login, Is_guest_login, Count, Srv_count, Serror_rate, Srv_serror_rate, Rerror_rate, Srv_rerror_rate, Same_srv_rate, Diff_srv_rate, Srv_diff_host_ rate, dst host count, dst host srv count, Dst_host_same _srv_rate, Dst_host_diff_ srv_rate, Dst_host_same_src_port_rate, Dst_host_srv_ diff_host_rate, Dst_host_serror_rate, Dst_host_srv_serror_rate, Dst_host_rerror_rate, Dst_host_srv_rerror_rat.

The detailed feature data types, attack types, Classes in NSL-KDD datasets, and preprocessing for dataset are shown in [25].

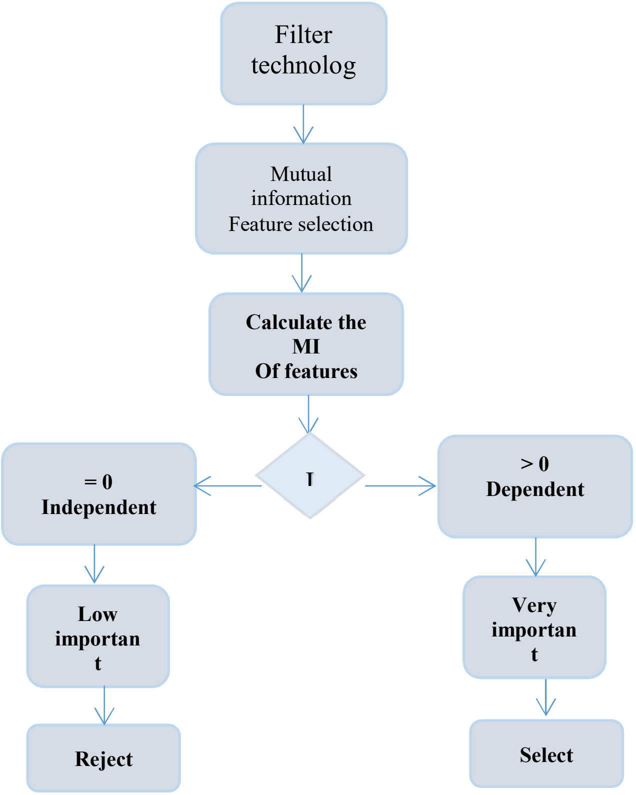

Fig. 3. Feature Selection algorithms

B. Feature selection

Feature selection is a widely utilized technology in DL and ML models that aims to optimizes the number of features by selecting the most related ones. Mutual information (MI) is extensively utilized in the field of DL and ML models, and is used to measure linear and nonlinear correlations [25]. Figure 3 show the feature selection steps.

C. Split the dataset into a training and testing set

The dataset in the anomaly-based IDS using the DL model was split as the following table:

TABLE I. THE NSL-KDD DATASET SPLIT IN THE PROPOSED DL MODE

NSL-KDD dataset = 148517	
Training 80%	**Testing 20%**
118813	29704

III. DEEP NEURAL NETWORK (DNN) CLSSIFICATION ALGORITHM

DNN is a feed-forward neural network, which is one of the modern methods for producing satisfactory and good results in the classification process and in which the signal entering the network is always directed forward. Thus, the outgoing signal from any neuron depends only on the incoming signal. Forward-feeding neural networks need the presence of two pairs of vectors, which are the required input and output vectors. An essential part of building a DNN is the utilization of powerful and accurate learning algorithms. The back propagation algorithm is one of the most important algorithms used in training a DNN. The training of the DNN by backpropagation includes three stages: feed-forward to the input training models, computation, and backpropagation of associated errors and weight adjustment. In training, there is input and output, where the inputs are processed, the resulting outputs are compared against the desired outputs, and on the basis of that comparison, errors are calculated and published back in order for the algorithm to adjust the weights.

This process is repeated, and with it, weights are constantly altered. The training set is the collection of data that makes training possible. The same set of training data is processed numerous times during a DNN training phase in order to properly change the weights. After training, the network application includes only feed-forward calculations.

The construction of DNN depends on the number of layers and the number of neurons in each layer, the activation function, and a training algorithm, which determines the weights' final value. In this search, a feedforward DNN was selected to build the classifier and to rely on a backpropagation algorithm to apply feedback to adjust weights during training. The equations for all layers are mentioned in detail in the following [18]:

Input layer: neurons number is determined by the total features number in a dataset. Inputs in the input layer are expressed as given in the following Equation 1:

$$X = [x\_1, x\_2, \ldots., x\_D] \qquad (1)$$

The hidden layers: Three layers were proposed with regard to the number of neurons in these layers; they were selected based on conducting several experiments and depending on the best results, where a number of neurons was 8 for two layers and 16 for one layer. The inputs of these layers are the outputs of an input layer, in addition to weights and biases.

Inputs in the hidden layer are expressed as given in the following Equation 2:

$$z_j = \sum_i w_i x_i + b_j \qquad (2)$$

We suggest using an activation function in each hidden layer, *ReLU* activation function is used in a processing process because it improves performance and accelerates the training process given in the following Equation 3:

$$R(z) = \max(0, z) \qquad (3)$$

Outputs in the hidden layer are denoted as given in the following Equations 4 and 5.

$$h = f(z_j) \qquad (4)$$

where *f(z$_i$)* is given by:

$$f(z_j) = \mathrm{ReLU}(z_j) \qquad (5)$$

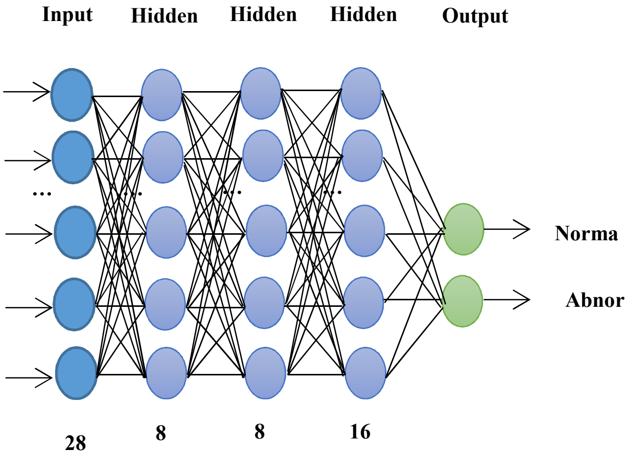

Fig. 4. DNN for binary classification

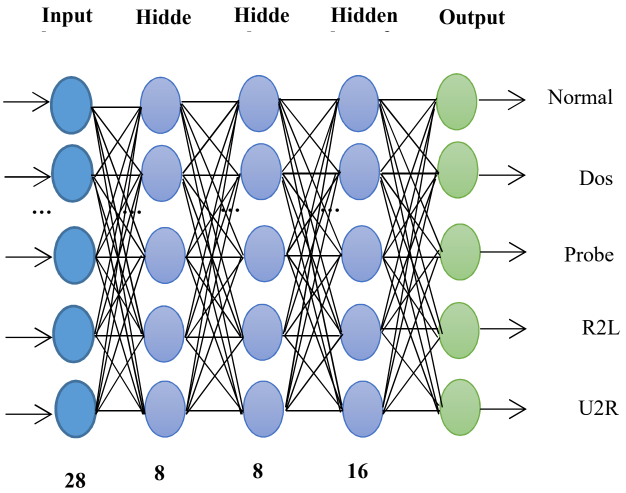

Fig. 5. DNN for multi-classification

Output layer: neurons number is determined by the classification result. In binary classification, one is either normal or abnormal, and in multiple classification, there are five, either normal or one of the four basic types of attacks. Its inputs are the outputs of hidden layers that are processed; we suggest using the activation function sigmoid for binary classification given in the following Equation 6:

$$S(z) = \frac{1}{1+e^{-z}} \qquad (6)$$

We suggest using the activation function ***softmax*** for multi-class classification given in the following Equation 7:

$$S(z_j) = \frac{e^{z_j}}{\sum_{k=1}^{k} e^{z_k}} \qquad (7)$$

This layer produces the outputs of the DNN. For example, Fig. 4 shows a DNN for binary classification and Fig. 5 for multiple classification.

IV. Experimental Results

In this section, the results obtained by the experimental study of the proposed model for IDS based on the DL algorithm are discussed.

A. Tools

Python implemented the proposed model using the Pandas, NumPy, and Scikit-Learn packages in the Anaconda platform, especially the Jupyter Notebook. Training and testing were carried out on a laptop computer with an Intel(R) Core (TM) i5-2430M CPU running at 2.40 GHz and 16 GB of memory running Windows 10. 5.3.3.

B. Experimental Inputs and Parameters

The dataset NSL-KDD was utilized as inputs for evaluation and analysis of the performance of the proposed model, which is distributed as follows in Tables II and III.

TABLE II. Distribution the dataset as input

Dataset	148517			
Training dataset	118813			
Testing dataset	29704			
Training dataset in binary classification				
Normal	**Attack**			
62803	**56010**			
Testing dataset in binary classification				
Normal	15785			
attack	13919			
Training dataset in multi-class classification				
Normal	**DOS**	**Probe**	**R2L**	
62893	43156	11082	1615	
Testing dataset in multi-class classification				
Normal	**DOS**	**Probe**	**R2L**	**U2R**
15695	10866	2731	389	23

TABLE III. Parameters for DL algorithms

Algorithms	**Parameters**	**Value**
DNN	Layers number	5
	Neurons number	Input layer :28
		Hidden layer :32
		Output layer : in binary classification : 1 in multi-classification :5
	Activation function	Relu,softmax,sigmoid
	Optimizer	Adam
	Loss	Binary_crossentropy Sparse_categorical_ Crossentropy
	The number of iterations	10

C. Evaluation metrics

Metrics to measure and evaluate the performance of a proposed model were used, including the confusion matrix, accuracy, precision, recall, and F1-score, which shows the relationship between true and false classified features.

Confusion matrix: The efficiency of a proposed model for intrusion detection is measured by its ability to detect intrusions correctly. The confusion matrix in Table VI is the most critical measure of the proposed model's performance. It expresses values resulting from my comparison between the nature of the event and the prediction the proposed model issued concerning the event itself.

TABLE IV. CONFUSION MATRIX

		Predicted Positive	**Predicted Negative**
		Normal	Attack
Actual Positive	Normal	True Positive (TP)	False Negative (FN)
Actual Negative	Attack	False Positive(FP)	True Negative (TN)

Equations 8, 9, 10, and 11, describe the calculations of accuracy, precision, recall, and F1-score respectively.

$$\text{Accuracy} = (\text{TP} + \text{TN})/.(\text{TP} + \text{TN}+.\text{FP} + \text{FN}) \quad (8)$$

$$\text{Precision} = \text{TP}/.((\text{TP} + \text{FP})) \quad (9)$$

$$\text{Recall.} = \text{TP}/.((\text{TP} + \text{FN})) \quad (10)$$

$$\text{F1\_Score} = 2 * (\text{precisio} * \text{recall.}/\text{precision} + \text{recall}) \quad (11)$$

D. Performance evaluation of binary classifier IDS using DNN algorithm

This classifier is typically based on the DL algorithm. The DNN algorithm is developed as a classifier, which is utilized to analyze whether network traffic is normal or an attack. The distributions of records in binary classification as "normal" or "attack" for both the training and testing datasets. Table V illustrates the evaluation metrics of the proposed model using the DNN algorithm.

TABLE V. THE ACCURACY, PRECISION, RECALL, AND F1-SCORE. USING DNN ALGORITHM

Accuracy	Precision	Recall	F1-score
0.9915	0. 99172698	0.991446065	0.991581715

E. Performance evaluation of multi-classifier IDS using DNN algorithm

For the training and testing, the distribution of records in the multi-class classification is normal and special attacks (DOS, Probe, R2L, and U2R).

The performance evaluation was tested on a testing dataset by classifying the data into five classes. The results of the proposed model evaluation using the DNN algorithm are shown in Table VI.

TABLE VI. THE ACCURACY, PRECISION, RECALL, AND F1-SCORE.USING A DNN ALGORITHM

Accuracy	**Precision**	**Recall**	**F1-score**
0.99181926250	0.99188246726	0.99882990121	0.9956848716

F. Performance result comparison of the proposed DL model and ML algorithms

The performance results of the proposed model using DNN algorithm and another model based on ML algorithms [25] in binary classification and multi classification are shown in Table VII, which summarize the results in terms of accuracy.

TABLE VII. THE ACCURACY OF THE PROPOSED MODEL USING DNN ALGORITHM AND ML ALGORITHMS

Algorithm	**Accuracy in binary classification**	**Accuracy in multi-classification**
Proposed DNN	0.9915	0.9918
RF [25]	0.9978	0.9974
SVM [25]	0.9898	0.9878

From Table VII, the experimental results show that the proposed model using DNN algorithm outperforms SVM algorithm in terms of accuracy. The RF algorithm outperforms the proposed model due to use the SMOT technique for dataset balance.

G. Performance result comparison of the proposed DL model and with the state-of-the-art DL algorithms

A comparison of the results in binary and multi-class classification, we have verified the superiority of the proposed model using DL algorithms (DNN) by comparing the accuracy with previous DL relevant works.

Binary classification: The proposed model using the DNN algorithm obtained accuracy 99.15%. While [7] proposed a model for IDS using the DNN algorithm and XGBoost technology for selecting features, and selected 16 features where it achieved an accuracy of 97%. Table VIII and Fig. 6 summarize the results of the proposed model classification using a DNN algorithm with other works that used the same dataset.

TABLE VIII. AN ACCURACY OF THE PROPOSED MODEL USING A DNN ALGORITHM AND OF RELATED PREVIOUS WORK

Algorithm	**Accuracy**
DNN [7]	97
DNN in the proposed model	**99.15**

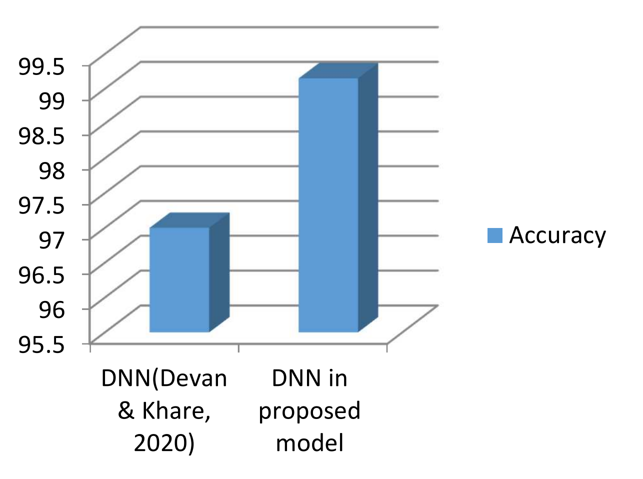

Fig. 6. an accuracy of the proposed model using DNN algorithm with related previous work in [7]

From the above figure and table, the experimental results display that the performance of the proposed model using

DNN algorithm outperforms previous relevant work by 2.15% enhancement in terms of accuracy.

Multi-classification: The proposed model using DNN algorithm obtained accuracy 99.18%, while [18] proposed an IDS using DNN and a cross-correlation approach to select features. Where it achieved an accuracy of 95.53%. Table IX and Fig. 7 summarize the results of the proposed model using DNN with the other work that used the same dataset and feature selection.

TABLE IX. AN ACCURACY OF THE PROPOSED MODEL USING A DNN ALGORITHM AND OF RELATED PREVIOUS WORK

Algorithm	Accuracy
DNN [18]	95.53
DNN in proposed model	**99.18**

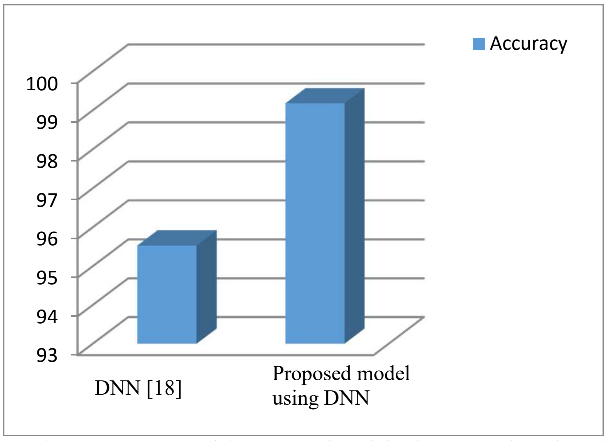

Fig. 7. an accuracy of the proposed model using DNN algorithm with related previous work in [18]

From Table IX and Fig. 7, it is clear that the performance results of the proposed model outperform other previous relevant works by 3.65% enhancement in terms of accuracy.

V. CONCLUSION AND FUTURE WORKS

The security of WSNs has recently emerged as a key source of concern, and the increase in attacks and threats against networks has become a severe problem that risks network security. In this paper, we addressed the problem of intrusion detection in WSNs, including the difficulty in determining the appropriate dataset, the drawbacks of feature selection, the imbalanced dataset, and the selection of the appropriate algorithm for the classification process. Thus, this paper proposed a model for anomaly-based IDS using DNN algorithm in WSNs, that analyzed the network traffic and applied the classification process. The two main contributions of the proposed model are: applying the MI technique for feature selection and conducting a comparative study using ML and DL algorithms. The results showed that the proposed model can enhance the performance of IDS using DL algorithms, and outperform the state-of-the-art by 3.5% in terms of accuracy. As the feature works, an IDS can be positioned at each sensor in the WSN and study their effect on energy consumption. Furthermore, the proposed model can be used in other systems, such as detecting cancers, detecting people with diabetes or heart disease, and classifying plant species.

REFERENCES

[1] Panahi, Uras, and Cüneyt Bayılmış. "Enabling secure data transmission for wireless sensor networks based IoT applications." Ain Shams Engineering Journal 14.2 (2023): 101866.

[2] Forster, Anna. *Introduction to wireless sensor networks*. John Wiley & Sons, 2016.

[3] Ashok Kumar, D., and S. R. Venugopalan. "A design of a parallel network anomaly detection algorithm based on classification." *International Journal of Information Technology* 14.4 (2022): 2079-2092.

[4] Ganeshan, R., and T. Daniya. "A systematic review on anomaly based intrusion detection system." *IOP Conference Series: Materials Science and Engineering*. Vol. 981. No. 2. IOP Publishing, 2020.

[5] Almomani, Omar. "A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms." *Symmetry* 12.6 (2020): 1046.

[6] Siddique, Kamran, et al. "Developing an intrusion detection framework for high-speed big data networks: A comprehensive approach." *KSII Transactions on Internet and Information Systems (TIIS)* 12.8 (2018): 4021-4037.

[7] Devan, Preethi, and Neelu Khare. "An efficient XGBoost–DNN-based classification model for network intrusion detection system." *Neural Computing and Applications* 32.16 (2020): 12499-12514.

[8] Shakya, Subarna, and Bisho Raj Kaphle. "Intrusion detection system using back propagation algorithm and compare its performance with self organizing map." *Journal of Advanced College of Engineering and Management* 1 (2015): 127-138.

[9] Gupta, Monika, and S. K. Shrivastava. "Intrusion detection system based on SVM and bee colony." *International Journal of Computer Applications* 111.10 (2015).

[10] Sumaiya Thaseen, I., et al. "An integrated intrusion detection system using correlation-based attribute selection and artificial neural network." *Transactions on Emerging Telecommunications Technologies* 32.2 (2021): e4014.

[11] Xu, Wen, et al. "Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset." *IEEE Access* 9 (2021): 140136-140146.

[12] Gurung, Sandeep, Mirnal Kanti Ghose, and Aroj Subedi. "Deep learning approach on network intrusion detection system using NSL-KDD dataset." *International Journal of Computer Network and Information Security* 11.3 (2019): 8-14.

[13] Choi, Hyunseung, et al. "Unsupervised learning approach for network intrusion detection system using autoencoders." *The Journal of Supercomputing* 75 (2019): 5597-5621.

[14] Li, Jie, et al. "Machine learning algorithms for network intrusion detection." *AI in Cybersecurity* (2019): 151-179.

[15] Ali, Mohammed Hasan, et al. "A new intrusion detection system based on fast learning network and particle swarm optimization." *IEEE Access* 6 (2018): 20255-20261.

[16] Shen, Yanping, et al. "An ensemble method based on selection using bat algorithm for intrusion detection." *The Computer Journal* 61.4 (2018): 526-538.

[17] Perez, Deyban, et al. "Intrusion detection in computer networks using hybrid machine learning techniques." *2017 XLIII Latin American Computer Conference (CLEI)*. IEEE, 2017.

[18] Gowdhaman, V., and R. Dhanapal. "An intrusion detection system for wireless sensor networks using deep neural network." *Soft Computing* 26.23 (2022): 13059-13067.

[19] Zhang, Wenjie, et al. "Wireless sensor network intrusion detection system based on MK-ELM." *Soft Computing* 24.16 (2020): 12361-12374.

[20] Otoum, Safa, Burak Kantarci, and Hussein T. Mouftah. "On the feasibility of deep learning in sensor network intrusion detection." *IEEE Networking Letters* 1.2 (2019): 68-71.

[21] Xiao, Xin, and Ruirui Zhang. "Study of immune-based intrusion detection technology in wireless sensor networks." *Arabian Journal for Science and Engineering* 42 (2017): 3159-3174.

[22] Sun, Xuemei, et al. "An integrated intrusion detection model of cluster-based wireless sensor network." *PloS one* 10.10 (2015): e0139513.

[23] Eesa, Adel Sabry, Zeynep Orman, and Adnan Mohsin Abdulazeez Brifcani. "A novel feature-selection approach based on the cuttlefish

optimization algorithm for intrusion detection systems." *Expert systems with applications* 42.5 (2015): 2670-2679.

[24] Obeidat, Ibrahim, et al. "Intensive pre-processing of kdd cup 99 for network intrusion classification using machine learning techniques." (2019): 70-84.

[25] Al-Fuhaidi, B., Farae, Z., Al-Fahaidy, F., Nagi, G., Ghallab, A., & Alameri, A. (2024). Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms. Applied Computational Intelligence and Soft Computing, 2024(1), 2625922.