Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.025669
Article

Tech Science Press

Wrapper Based Linear Discriminant Analysis (LDA) for Intrusion Detection in IIoT

B. Yasotha[1,*], T. Sasikala[2] and M. Krishnamurthy[3]

[1]Department of Computer Science and Engineering, MNM Jain Engineering College, Chennai, 600097, India
[2]Department of School of Computing, Sathyabama Institute of Science and Technology, Chennai, 600119, India
[3]Department of Computer Science and Engineering, KCG College of Technology, Chennai, 600097, India
*Corresponding Author: B. Yasotha. Email: byasothaa21@outlook.com
Received: 01 December 2021; Accepted: 08 April 2022

Abstract: The internet has become a part of every human life. Also, various devices that are connected through the internet are increasing. Nowadays, the Industrial Internet of things (IIoT) is an evolutionary technology interconnecting various industries in digital platforms to facilitate their development. Moreover, IIoT is being used in various industrial fields such as logistics, manufacturing, metals and mining, gas and oil, transportation, aviation, and energy utilities. It is mandatory that various industrial fields require highly reliable security and preventive measures against cyber-attacks. Intrusion detection is defined as the detection in the network of security threats targeting privacy information and sensitive data. Intrusion Detection Systems (IDS) have taken an important role in providing security in the field of computer networks. Prevention of intrusion is completely based on the detection functions of the IDS. When an IIoT network expands, it generates a huge volume of data that needs an IDS to detect intrusions and prevent network attacks. Many research works have been done for preventing network attacks. Every day, the challenges and risks associated with intrusion prevention are increasing while their solutions are not properly defined. In this regard, this paper proposes a training process and a wrapper-based feature selection With Direct Linear Discriminant Analysis LDA (WDLDA). The implemented WDLDA results in a rate of detection accuracy (DRA) of 97% and a false positive rate (FPR) of 11% using the Network Security Laboratory-Knowledge Discovery in Databases (NSL-KDD) dataset.

Keywords: Intrusion detection; IIoT; wrapper; support vector machine (SVM); LDA; random forest (RF); feature selection

1 Introduction

Intrusion has become a severe issue in the provision of security for network traffic. A single instance of intrusion can hack, steal or even damage data from both computer and network systems, and could potentially harm its hardware. In addition, intrusion can create huge losses in the field of IIoT. Consequently, the processes of detecting and preventing intrusions have become vital in an IIoT

environment [1]. Since all industries have been connecting to one another, sharing valuable information in an intelligent way requires the Industrial Internet of Things (IIoT). Through the IIoT platform, many industries operate in various domains such as a smart city, smart power management, automation, logistics, supply chain process, and health care [2]. Through different sensor signals, an IIoT communicates and maintains the established infrastructure, sharing valuable information through a larger network. The aim of the IIoT is to facilitate the intelligent production and delivery of goods by establishing in smart companies effective communication between customers and business dealers [3]. Industry 4.0 has focused on the implementation of an optimized problem for utilizing smart devices through data-driven services. The resulting intelligent activities achieve efficient work by seamlessly connecting together various smart devices. In order to carry out that process, a reliable uninterruptable network connecting the smart devices is required. Through this network connection, cyber-attacks might occur threatening the smart industries in various ways. Hackers also try to get sensible information in the IIoT environment. Therefore, an industrial control system is needed to control the intelligent activities of smart devices [4]. Detecting the vulnerabilities in the traffic of the network in IIoT is called an Intrusion detection system. To provide security in IIoT, the initial step is to identify the hackers, network traffic, security logs, collect information from the system point of view to check for the damages in the network [5].

The process of preventing hackers in IIoT needs customized solutions with smart devices connected to the network. Its applications need deep learning or machine learning techniques for improving the efficiency and low-cost maintenance in the IIoT field. Moreover, various research works have been explored in accordance with IDS in IIoT. The main drawbacks of the existing techniques are time consumption and inefficiency. To overcome these issues, this paper describes the pre-processing technique and implements sterilization and normalization. In order to improve the accuracy, it has adopted wrapper-based direct LDA, and for classification, optimized Extreme Learning Machine (ELM) with Particle swarm optimization (PSO) is applied for relevant features. In the research, it is tried in responding to the following research questions comprehensively:

Q1: How does the proposed feature selection algorithm wrapper-based direct LDA technique outperform after comparing it with the existing work?

Q2: How far the optimized algorithm of Particle Swarm Optimization (PSO) with Extreme Learning Machine (ELM) are the efficient ones?

For intrusion detection systems, the machine learning algorithm of the Naive Bayes algorithm (NB) is used to detect intrusion [6]. This algorithm is utilized for reducing the feature of the original data feature. NB is used for intrusion detection in the aspects of the accuracy and reducing the features.

The Logistic Regression algorithm (LR) was implemented in the evaluation of mapping features of data. In this LR method, it selected 23 features to create a new dataset [7]. The main contributions of this research work are listed below.

1. Implementation of machine learning-based IDS model for different industrial IIoT applications.
2. Use of optimized ELM with PSO for classifying the intrusions.
3. Selection of relevant features using wrapper-based direct LDA.

The research work has been organized as follows: Section 2 elaborates the review of the literature, Section 3 describes the selection of features using wrapper based direct LDA, Section 4 discusses the feature classification, Section 5 shows the evaluation of results and Section 6 presents the conclusion about the research work with future predictions.

2 Review of Literature

The main aim of IDS is to detect, observe and prevent the intruder's attack in IIoT or interconnected network or node. It acts as a protector and also it safeguards the network node or IIoT from intruders [8]. Sensor nodes are used to identify malicious activities. Similarly, IDS can monitor the actions of the user and determine the behavior of hackers as well as a malicious network node. In the paper [9], different classifier algorithms were implemented with the NSL-KDD data set. It analyzed the protocols by using the WEKA tool for detecting the intruders in the network. For improving the accuracy, dimensionality reduction-based Chronic Fatigue Syndrome (CFS) was used. IDS system monitored the actions of the user to check whether the attack was normal or malicious behavior. In that regard, three types of IDS were used. They were Host-based IDS System (HIDS), Anomaly-based IDS System (AIDS), Network-based IDS System (NIDS) [10].

In the paper [11], the NB15 dataset had introduced a new hybrid model for IDS and monitored each attack using Support Vector Machine (SVM) and Genetic Algorithm (GA). Least Square Support Vector Machine (LS-SVM) based IDS was proposed in the paper [12]. Feature selection-based information concept was used for handling linear and non-linear features of correlation. They used various datasets of KDD cup 99, NSL-KDD, and Kyoto 2006+. For feature reduction in the data set of NB15, Random Forest (RF) was implemented in order to monitor the attack of "Fuzzers". False Alarm Rate (FAR) and non-detection of data were performed [13]. Deep learning methods had also been implemented for the detection of the multiclass approach based on anomaly detection. In that case, Convolutional Neural Network (CNN) was used in the form of 8 × 8 images which were to be entered into CNN layers for the classification of accuracy [14]. Tab. 1 shows the survey of the existing algorithm in IDS.

Table 1: Survey on IDS

Author name	Technique used
Khraisat et al., 2021 [15]	IDS with (Internet of Things) IoT.
Chauhan et al., 2020 [16]	IDS in IoT.
Alazzam et al., 2020 [17]	Feature reduction-based technique called Pigeon Inspired Optimizer (PIO)
Almomani, 2020 [18]	Feature extraction using optimized algorithms of Genetic Algorithm (GA), Particle Swarm Optimization Algorithm (PSOA), Firefly Optimization Algorithm (FOA), and Grey Wolf Optimization (GWO).
Hammad et al., 2020 [19]	Used Correlation-based Feature Selection (CFS), Random Forest (RF), Naive Bays (NB), Random Forest (RF), J48. Also, K-MEANS and Expectation Maximization (EMC) Clustering-based methods
Kasongo et al., 2020 [20]	Filter-based feature selection Extreme Gradient Boosting (XG) Boost.
Yin et al., 2017 [21]	Recurrent Neural Network (RNN)
Misiko et al., 2017 [22]	IDS
Khammassi et al., 2017 [23]	Genetic algorithm with Logistic regression-based feature selection
Mehmod et al., 2016 [24]	Feature selection-based Ant Colony Optimization (ACO)

3 Proposed Wrapper Based LDA Methodology

In the anomaly detection of IIoT using IDS, dual feature selection of LDA and Principle Component Analysis (PCA) with wrapper-based algorithm were used in the training process. This work was

implemented using four phases such as pre-processing, feature selection, feature classification with the optimized algorithm, and ensembled the processing. Initially, the data set was categorized into two sets such as training and testing with the ratio of 8:2. For the sake of improving the accuracy level, pre-processing was needed in the aspect of balancing the data and handling the missing values and irrelevant values. Fig. 1 shows the architecture of the proposed work.

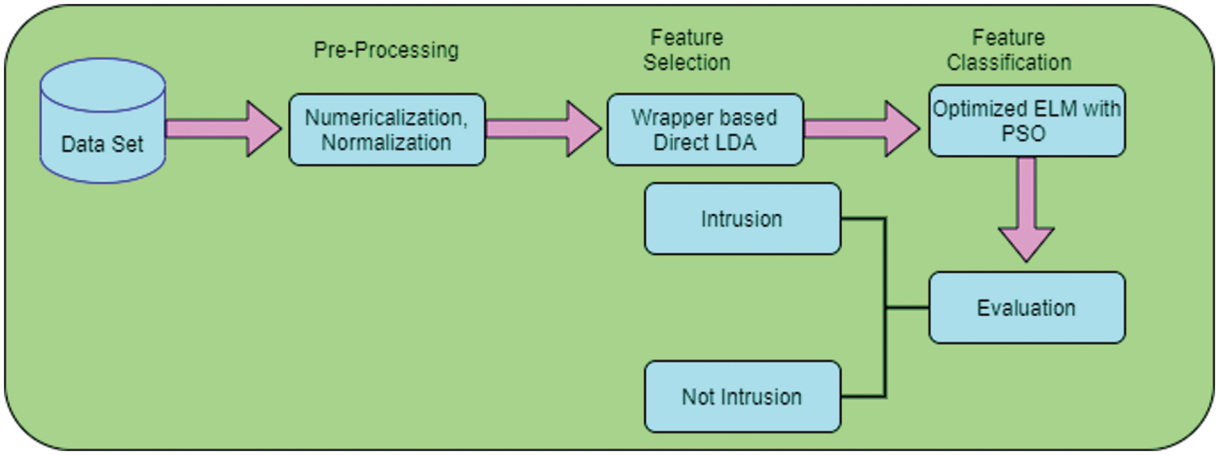

Figure 1: Architecture of proposed work

In this work, sterilization and normalization were included in the pre-processing phase. In the sterilization, the noise values were replaced with null or infinity symbols. In the normalization, all feature values were brought to the same scale. In the proposed work, wrapper-based feature selection and deep feed-forward neural network model were considered. This procedure was used to reduce the number of features for further proceeding. Artificial neural network, filtered-based SVM, RF, and Decision Tree (DT) were used in the classifiers.

3.1 Pre-Processing

Due to the large volume of traffic in the network to detect the intruders, the raw input data from the dataset are found to be intricated to process with all the features. These raw data may consist of either numeric or non-numeric data. These input data are needed to be pre-processed using numericalization and normalization.

3.1.1 Numericalization

For handling the noise values, numericalization is used, which replaces the values of noise win th infinity symbols of mean values or zero values.

3.2 2 Normalization

In the dataset, the input data attributes are in unstructured format such as numeric or non-numeric data. To consider all input data attributes in the uniformity scale, normalization is used. The normalization procedure is defined by min-max procedure, Within the range interval of [−3,3]

$$Y = -3 < \min(x_{max}, \max(x, x_{min})) < 3 \tag{1}$$

Standardization is represented as

$$x_i = \frac{Y - \mu}{\sigma} \tag{2}$$

where, mean (μ) is defined as:

$$\mu = \frac{1}{N}\sum_{i=1}^{N}(Y_i) \tag{3}$$

The standard deviation σ is defined as:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(Y_i - \mu)^2} \tag{4}$$

After pre-processing, each record in the NSL-KDD dataset contains 100 dimensions.

3.3 Feature Selection using Proposed Wrapper Based Direct LDA Model

In the feature selection process, from the input features d of data set, the relevant features r are considered for getting more optimized result i.e., $r < d$. This work has implemented the wrapper method of bidirectional elimination with direct LDA (Linear Discriminant Analysis) for feature selection. The bidirectional elimination wrapper method is similar to the forward selection technique. The steps involved in bi-directional elimination are as follows:

Algorithm 1 Implementation of wrapper method for feature selection

Input: Input dataset DS with features, number of data

Output: Reduced features with a normalized data set

Step 1: Select threshold value $thresh = 0.05$

Step 2: Choose feature of the dataset with minimum $p - value$

Step 3: Apply fitness to that feature and add one more feature with minimum $p - value$

Step 4: If $p - vlaue < thresh$ go to step 2

Step 5: Else

Step 6: Choose feature of the dataset with maximum $p - value$

Step 7: Apply fitness to that feature and choose one more feature with maximum $p - value$

Step 8: if $p - vlaue > thresh$ go to step 6

Step 9: Remove that feature from the dataset

Step 10: Else

Step 11: Repeat steps 2 to 9 until getting an optimal set of features from the dataset.

In wrapper methods, the feature selection process is based on a Direct Linear Discriminant Analysis (DLDA) algorithm. The steps involved in the wrapper method contain three techniques such as forward selection in which the p-value is less than the threshold value and is added. The next technique is backward elimination from the features in the dataset, in which the p-value is greater than the threshold value and is removed from the dataset. The procedures involved in DLDA are explained below:

Algorithm 2: Wrapper Based Direct Linear Discriminant Analysis (DLDA)

Input: Reduced input feature data set

Output: Optimal discriminant matrix Q *with* relevant features.

Step 1: Implement Algorithm 1 to select features from the raw input data set using the wrapper method. For getting an optimized features space by using DLDA is applied.

Step 2: Replace the null space ds_{values} by zero eigenvalues.

Step 3: Use diagonal values of ds_{values} generate eigen vectors.

Step 4: Generate the matrix M, such that $M^T ds_{values} M = \Lambda_{values}$, here Λ_{values} is a diagonal matrix with non-zero eigen elements and it is sorted by descending order M *contains* eigen vectors.

Step 5: Let $N = M\Lambda_{values}^{-1/2}$, by using eigen vector values generate discard space. Now the eigen value of matrix is defined as $N^T ds_w N$, such that $P^T(N^T ds_w N)P = \Lambda_{values}$. Here P is the discarded space and Λ_{values} is a diagonal matrix.

Step 6: Evaluate the optimal discriminant matrix $Q = NP\Lambda_{vlaues}^{-1/2}$. The value of matrix Q contains reducing the high dimensionality of the data space into low dimensionality of feature space.

The wrapper method is implemented with Direct Linear Discriminantt Analysis (DLDA). An elegant dimensionality reduction is an essential one for making a feature in the database. This reduction in dimensionality is used to reduce the features of input data into low dimensionality of feature space.

In the DLDA algorithm, replacement of null spaces by its zeeigenvaluesues and generation of eigen vectors using null space of he features in the data set are carried out. The optimal discriminant matrix Q which satisfies:

$$Q^T ds_w A = Id,\ Q^T ds_{values} Q = \Lambda \tag{5}$$

Here Id is the identity matrix and Λ is the diagonal matrix with elements in decreasing order. Further ds_{values}, ds_w are between class matrix and within class matrix of the dataset.

3.4 Feature Classification

From the feature selection process, the optimal relevant features are selected for classifying the intrusive type of data and normal data. This method is called an intrusive analytical engine. Feature classification is an important stage for detecting the malicious attacks in IIoT. This paper has proposed Extreme Learning Machine (ELM) with Particle Swarm Optimization (PSO) method for detecting the intrusion in IIoT IDS.

3.4.1 Extreme Learning Machine Model (ELM)

The basic concept of ELM is based on single or multiple hidden layer feed forward neural network [25]. The structure of ELM consists of input, one or more multiple layers and output layer. In order to get an accurate and effective detection of intrusion, weight adjustment between input and hidden layer is needed. The comparison and weight adjustment are based on the Single Layer Feed Forwards (SLFN) Neural Network. Fig. 2 shows the architecture of ELM based SLFN.

Fig. 2 shows the choice of M sample relevant features from the data set using Algorithm 2 and the select (r_i, q_i), where $r_i = [p_{i1}, p_{i2}, \ldots p_{in}]^T$ is the i^{th} data with n various features and $q_i = [q_{i1}, q_{i2}, \ldots q_{in}]^T$ describes the labels of p_i with n hidden neurons and it is defined as:

$$\sum_{n=1}^{k} \beta_i h(w_n p_i + c_n) = \alpha_i,\ i = 1, 2, \ldots, M \tag{6}$$

where, $w_n = [w_{n1}\ ,\ w_{n2},\ w_{n3},\ \ldots,\ w_{nk}]^T$ is the weight vector with i^{th} neuron in the hidden layer with corresponding input nodes. $\beta_i = [\beta_{i1}\ ,\ \beta_{i2},\ \ldots, \beta_{in}]^T$ are the weight vector values of i^{th} neuron in the hidden layer with corresponding output nodes. c_n is the threshold value of i^{th} neuron in the hidden layer. $\alpha_i = [\alpha_{i1}\ ,\ \alpha_{i2},\ \ldots, \alpha_{in}]^T$ is the i^{th} output neuron and h is the activation function.

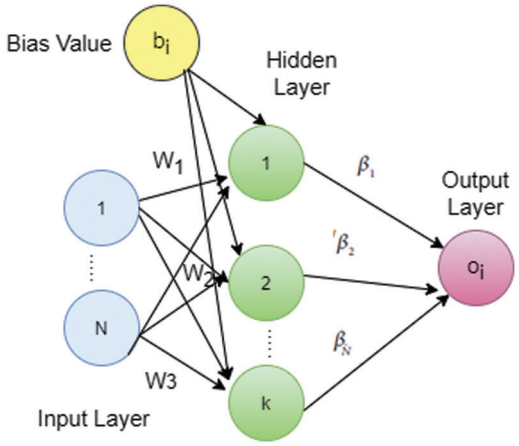

Figure 2: ELM for IDS

3.4.2 Particle Swarm Optimization (PSO)

The optimized algorithm of particle swarm optimization is an intelligence concept based on the global search system [25–27]. It is also called a reasonable algorithm because of its classifying detection of intrusion activities, computational reasonability, and global search [28]. Fig. 3 shows the PSO steps for classifying the intrusion activities in IIoT.

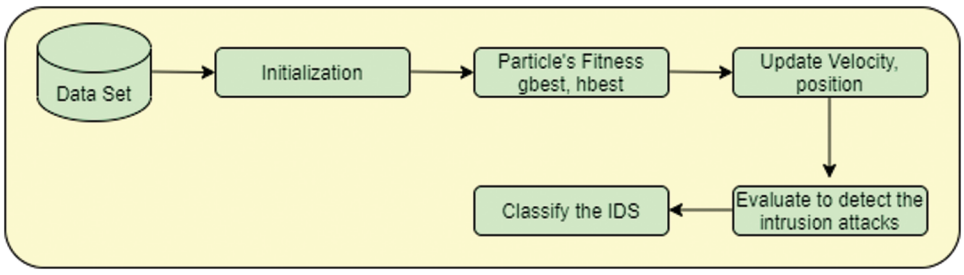

Figure 3: PSO for classifying IDS

By the selected features, PSO uses the principal space for classifying the intrusion activities in IIoT. In the PSO technique, space particles' population which is called as swarm is used for representing the solutions. For classifying the malicious attack in IIoT, the search space particles of 1 or 0 are randomly generated. If the space component in the principal is 1, the particle is chosen as no intrusive activities and if it is 0, the intrusive activities are ignored. In order to make it more powerful, the principal searching space is randomly traversed and optimal classification of IDS in IIoT is obtained. Velocity and position in the search space should be updated, and the position of the particle is given as:

$$p_i = \{p_{i1}, p_{i2}, \ldots, p_{iD}\} \tag{7}$$

$$vex_i = \{ve_{i1}\ ,\ ve_{i2},\ \ldots, ve_{iD}\} \tag{8}$$

Here D indicates particle search space. Position and velocity for search space are calculated as:

$$ve_{id}^{t+1} = w * ve_{id}^{t} + c_1 * r_{i1} * \left(p_{bid} - x_{id}^{t}\right) + c_2 * r_{i2} * \left(p_{gbd} - x_{id}^{t}\right) \tag{9}$$

Here D is the dimension and t represents the number of iterations for the search space. W is the value of weight and c1 and c2 are the constant values, r_{i1} and r_{i2} are randomly distributed values of 0 and 1. p_{bid} and p_{gbd} are dimension space. Values of location for each particle should be updated. The process is repeated until it reaches the maximum iteration or satisfies the fitness values. The algorithmic steps of PSO is given below:

Algorithm 3: Classification of IDS using PSO

Input: Relevant features input raw data set

Output: Detecting Intrusive activities

Step 1: Initialize the parametric values of fitness and number of particles

Step 2: Initialize the population pop_{i-best}

Step 3: For $(i = 1\ to\ N)$

Step 4: If fitness $x_{id}^{t} > fitnesspop_{i-best}$

Step 5: Update $pop_{i-best} = x_{id}^{t}$

Step 6: If fitness $x_{id}^{t} > g_{best}$

Step 7: Update velocity and position of particle

Step 8: End if

Step 9: End if

Step 10: End For

Algorithm 3 shows the dimensionality reduction of features which has improved the accuracy of classification in exploring the malicious attacks. At the same time, it has produced accurate and efficient results in detecting the intruders around IIoT [29–31].

4 Results and Discussion

This section discusses the analysis of the experimental study based on the proposed techniques in the selection of features and classifications of IDS.

4.1 Dataset Description

The dataset contains both normal and intruders' data in IIoT using NSL-KDD, [29]. The NSL-KDD dataset contains unbalanced distribution of data with large number of repeated data. The experiment is carried out by using two sets of data such as training and testing data set from NSL-KDD data set. There are 41 features which are divided into three types of features namely, symbolic features, binary features and continuous features. Specifically, the training data set contains 22 attacks and the testing data set contains 37 various attacks [32]. There are five classes in the data set. They are Probe, Normal, User to Root (U2R), Remote to Local (R2L), and Denial of Service (DoS) [33]. IDS attacks in IIoT with a detailed description in terms of training, testing data are mentioned in Tab. 2.

Table 2: IDS attacks in IIoT using NSL-KDD data set

Class	Attack	Attack types	Description	NSL-KDD dataset	
				Training Data	Testing Data
Normal pattern	No attack		Normal connection	67443	9610
Abnormal pattern	Denial of service	Udpstorm, the-Back, in-Land, Neptune, Pod, Smurf, Teardrop, Apache2, Processtable, Worm (totally 10 attacks)	This type of attackers makes the network resources as down as well as increase the network bandwidth. This automatically violates the data availability	46937	7568
	Probe (6 Attacks)	Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint (6 attacks)	Intruders try to collect the IIoT information. It will violate the rule to save the confidential data	11654	2633
	R2L (16 attacks)	_Guess_Password, _Ftp_write, -Imap, _Phf, _Multihop, _Warezmaster, _Warezclient, _Spy, _Xlock, _Xsnoop, _Snmpguess, _Snmpgetattack, _Httptunnel, _Sendmail, _Named (16 attacks)	Intruders make traffic flow and illegal access of data.	985	2878
	U2R (7 attacks)	Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps (7 attacks)	Obtain the root of PC. This also violates the integrity of the system.	62	87

4.2 Features Selection using Wrapper Based Direct LDA Model (WDLDA)

The NSL-KDD dataset consists of 41 features which are represented in Tab. 3. The proposed approach of the feature selection called WDLDA which has selected five relevant features from the feature set and it has improved the accuracy in the classification. This proposed approach is compared to the other existing feature selection techniques which is given in Tab. 4. And the selected features along with the name of the proposed techniques are given in Tab. 5.

Table 3: NSL-KDD dataset features

Feature number	Name of the feature	Feature number	Name of the feature
1	_Duration (fe1)	22	_Is_guest_login (fe22)
2	_Protocol_type (fe2)	23	_Count (fe23)
3	_Service (fe3)	24	_Srv_count (fe24)

(Continued)

Table 3 (continued)

Feature number	Name of the feature	Feature number	Name of the feature
4	_Flag(fe4)	25	_Serror_rate (fe25)
5	_Src_bytes (fe5)	26	_Srv_serror_rate (fe26)
6	_Dst_bytes (fe6)	27	_Rerror_rate (fe27)
7	_Land (fe7)	28	_Srv_rerror_rate (fe28)
8	_Wrong_fragment (fe8)	29	_Same_srv_rate (fe29)
9	_Urgent (fe9)	30	_Diff_srv_rate (fe30)
10	_Hot (fe9)	31	_Srv_dif_host_rate (fe31)
11	_Num_failed_logins (fe10)	32	_Dst_host_count (fe32)
12	_Logged_in (fe11)	33	-Dst_host_srv_count (fe33)
13	_Num_compromised (fe12)	34	_Dst_host_same_srv_rate (fe34)
14	_Root_shell (fe13)	35	_Dst_host_diff_srv_rate (fe35)
15	Su_attempted (fe15)	36	Dst_host_same_src_port_rate (fe36)
16	Num_root (fe16)	37	Dst_host_srv_dif_host_rate (fe37)
17	Num_file_creations (fe17)	38	Dst_host_serror_rate (fe38)
18	Num_shells (fe18)	39	Dst_host_srv_serror_rate (fe39)
19	Num_access_files (fe19)	40	Dst_host_rerror_rate (fe40)
20	Num_outband_cmds (fe20)	41	Dst_host_srv_rerror_rate (fe41)
21	İs_hot_login (fe21)	42	Class label (fe42)

Table 4: Feature selection of various techniques

FS approaches	No of features	Selected features
All features	41	fe1,fe2,fe3,fe4,fe5,fe6.fe7,fe8,fe9,fe10,fe11,fe12,fe13,fe14, fe15,fe16,fe17,fe18,fe19,f2e0,fe21,fe22,fe23,fe24,fe25, fe26,fe27,fe28,fe29,fe30,fe31,fe32,fe33,fe34,fe35,fe36, fe37,fe38,fe39,fe40,fe41
Flexible mutual information based feature selection [32]	18	fe5, fe30, fe6, fe3, fee4, fe29, fe12, fe33, fe26, fe37, fe39, fe34, fe25, fe38, fe23, fe35, f3e6, fe28
Flexible Linear Correlation Coefficient based Feature Selection [32]	22	fe29, fe12, fe33, f39, fe4, fe23, fe34, fe25, fe26, fe38, fe8, fe35, fe19, f32, fe18, fe3, fe6, f4e0, fe30, fe5, fe27, fe22
Synthetic Minority Oversampling Technique-ENN [33]	6	fe3, fe5, f3e0, fe4, fe6, fe29
Proposed WDLDA	5	fe3, fe5, fe30, fe4, fe29

Table 5: Selected feature names by WDLDA

Selected feature	Name of the feature
fe3	_Service
fe5	_Src_bytes
Fe30	-Diff_srv_rate
fe4	_Flag
fe29	_Same_srv_rate

4.3 Evaluation of Performance of Metric Measures

The experimental results of the proposed work are given using metric measures.

Detection Accuracy (DA):

It is the ratio of exact matching detections over the total number of instances in IDS evaluations.

$$DA = \frac{TP + TN}{TP + FP + TN + FN} \tag{10}$$

Error Rate (ER):

It measures the ratio of incorrect detections of malware attacks over the total number of cases. It is also called as misclassification of error.

$$ER = \frac{FP + FN}{TP + FP + TN + FN} \tag{11}$$

Mathews Correlation Coefficient (MCC)

It is a correlation between predicted output with the real data.

$$MCC = \frac{(TP.TN) - (FP.FN)}{\sqrt{(TP + FP).(TP + FN).(TN + FP).(TN + FN)}} \tag{12}$$

4.4 Performance Evaluation of Feature Selection using NSL-KDD Data Set

The performance of IDS is based on the real input features and the selected features are represented in Tab. 6. The real 41 features, normalized 41 input features and feature selection using WDLDA selected 5 features are given. The Tab. 6. shows the results which has proved the important of two steps in the process of normalization. It is used to avoid the traffic in the network data. The selection of feature process also overcomes the overfitting issue by enhancing the overall IDS performance in order to improve the classification in an accurate way. It has decreased the rate of error and the time for detection and also minimized the computational time complexity.

The performance of the selected features in the proposed work is compared with the existing techniques on IDS such as standard Flexible Mutual Information-based Feature Selection (FMIFS), Flexible Linear Correlation Coefficient based Feature Selection FLCFS [34] and Synthetic Minority Oversampling Technique-ENN [35]. The experimented results are shown in Tab. 7.

From the Tab. 7, it is clear that the proposed WDLDA feature selection has produced better performance when compared to the other techniques. The use of selected features have improved the classification in an accurate way so as to protect the IIoT from the attackers.

Table 6: Performance evaluation of the proposed feature selection algorithm

Evaluation metrics	Input features		
	Original features	Normalized features	Selected features by WDLDA
No of selected features	41	41	5
Detection Accuracy	91.43	95.67	97.91
FPR	0.018	0.014	0.010
FNR	0.187	0.061	0.015
Recall (%)	86.31	96.31	97.21
Training time (s)	252.39	15.023	3.53
Testing time (s)	266.1	42.31	8.03

Table 7: Performance evaluation of proposed WDLDA feature selection with other techniques

Metrics	Feature selection techniques			
	FMIFS	FLCFS	Synthetic Minority Over-sampling Technique (SMOTE)-Edited Nearest Neighbor (ENN)	Proposed WDLDA
Selected Features	18	22	16	5
MCC	0.18	0.31	0.22	0.14
Sensitivity	86.05	91.28	92.56	97.88
Specificity	90.23	91.27	87.16	98.12
Precision (%)	88.45	91.12	92.72	98.56

4.5 Performance Evaluation of Proposed WDLDAIDS with Existing IDS Systems

For proving the proposed work WDLDA based IDS system, it is compared with the existing IDS systems such as DM-Naive Bayes (DMNB) [36], Deep Belief Network (DBN)-SVM [37], Particle Swarm Optimization (PSOM) [38] and Synthetic Minority Oversampling technique-ENN. The evaluated results are shown in Tab. 8.

Table 8: Performance evaluation of various existing *vs.* proposed IDS systems

IDS systems	No. of selected features	Accuracy (%)	FPR
DMNB	41	95.01	1.76
DBN-SVM	41	93.53	2.03
PSOM	10	92.34	3.12
SMOTE-ENN	6	94.12	0.52
Proposed WDLDA -ELMPSO	5	97.71	0.11

From the experimental results, the Proposed WDLDA -ELM based Particle Swarm Optimizer (PSO) in IIoT IDS has obtained accuracy rate which is high and low of FPR rate. The proposed system obtains 97.71% of accuracy rate on the basis of detecting the intruders and 0.11 of False Positive Rate.

The WDLDA-ELMPSOIDS gets high accuracy because of the optimization process. Fig. 4 shows the Receiver Operating Characteristic Curve (ROC) curve for the analysis of accuracy rate of feature selection and elimination of redundant features from the data set. This is compared with the other existing techniques of DM-Naive Bayes (DMNB), Deep Belief Network (DBN)-SVM, Particle Swarm Optimization (PSOM) and Synthetic Minority Oversampling Technique-ENN.

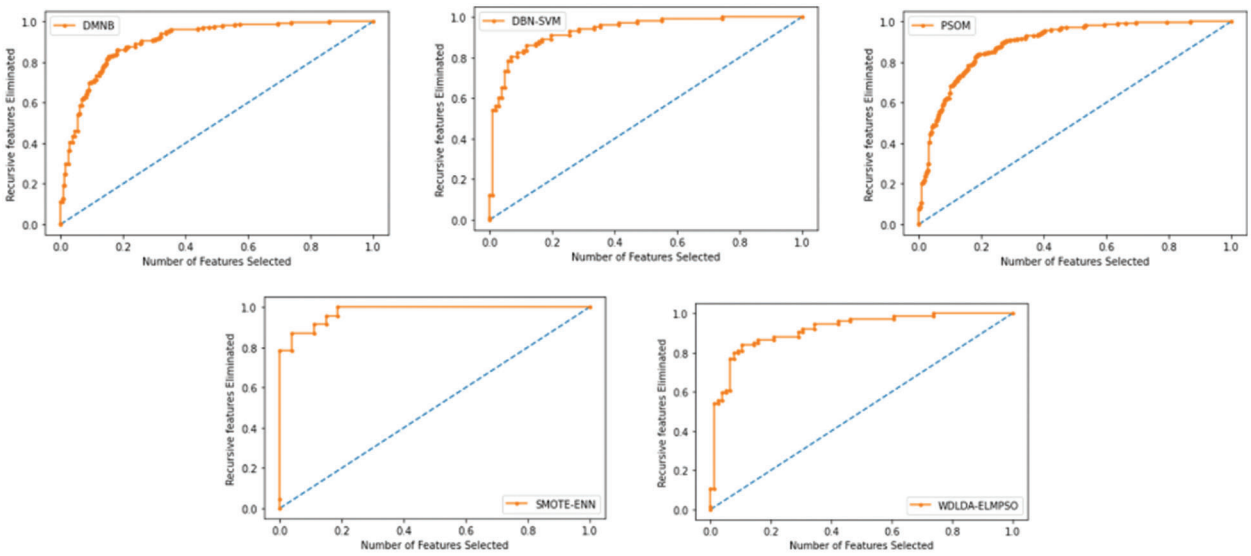

Figure 4: Elimination of recursive features

From the analysis of Fig. 4, it is observed that the proposed work has produced a significant improvement in the accuracy rate by selecting the features using WDLDA. Fig. 5 shows the false positive rate and true positive rate of the proposed work WDLDA-ELMPSO that is compared with the other exiting techniques.

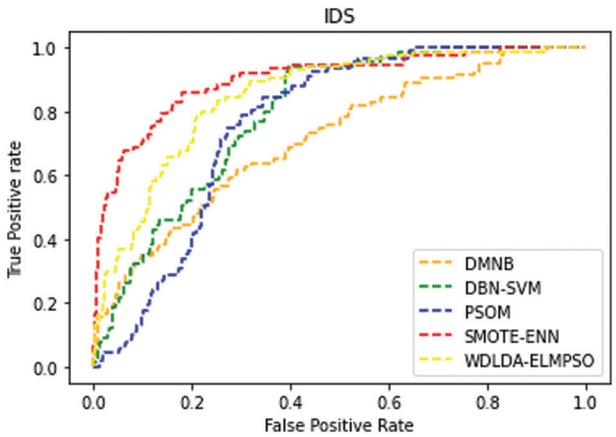

Figure 5: ROC for FPR & TPR

Intrusion Detection System (IDS) approach is used to identify the malicious intruder of information in IIoT. The proposed work has produced the better performance in the aspects of sensitivity and specificity and also produced exact classification in an accurate way, minimizing the rate of error, and reducing the

computational time complexity. Additionally in this work, the optimization algorithm is included so as to increase the accurate classification.

5 Conclusion

An improved wrapper-based feature selection with direct LDA has been proposed in this work for IDS. The usage of IIoT has increased and detected the malicious attacker in an efficient way. Handling the large number of features from the data set gives an inaccurate classification. Therefore, the proposed work WDLDA-ELMPSO is implemented with reduction of features using optimized deep learning algorithm which prevents the intruders in the traffic of network data. The advantage of the proposed work has high detection rate in accuracy. Also, it needs less computation and training time. In the analysis of the result, the proposed work WDLDA-ELMPSO has produced a better result when compared to the existing system. From the results, it is concluded that the accuracy is recorded as 97.71% and the false positive rate is recorded as 0.11 respectively. In future work, the usage of IIoT scheme could be increased and so it is necessary to provide detection of intruders in the traffic of the network by the improved version of various deep learning algorithms.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare no conflict of interest regarding the publication of the paper.

References

[1] M. Ahmad, M. J. Basheri and A. Rahim, "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection," *IEEE Access*, vol. 6, pp. 33789–33795, 2018.

[2] X. Ch, S. Latif, Z. Idrees, Z. Zou and J. A. Drann, "A deep random neural network model for intrusion detection in industrial IOT," in *Proc. Int. Conf. on UK-China Emerging Technologies (UCET)*, China, pp. 1–4, 2020.

[3] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "Ton IOT telemetry dataset: A new generation dataset of IOT and IIOT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

[4] T. Vaiyapuri, Z. Sbai, H. Alaskar and N. A. Alaseem, "Deep learning approaches for intrusion detection in IIoT networks opportunities and future directions," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, 2021.

[5] T. Vaiyapuri and A. Binbusayyis, "Application of deep auto encoder as an one-class classifier for unsupervised network int-rusiondetection: A comparative evaluation," *PeerJ Computer Science*, vol. 6, pp. e327, 2020.

[6] S. Mukherjee and N. Sharma, "Intrusion detection using naive bayes classifier with feature reduction," *Procedia Technology*, vol. 4, no. 7–8, pp. 119–228, 2012.

[7] B. Subba, S. Biswas and S. Karmakar, "Intrusion detection systems using linear discriminant analysis and logistic regression," in *Proc. IEEE Indicon*, New Delhi, India, pp. 1–6, 2015.

[8] L. Dhanabal and S. P. Shantharadah, "A study on NSLKDD dataset for intrusion detection system based on classification algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 446–452, 2015.

[9] M. A. Ambusaidi, X. He, P. Nanda and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016.

[10] A. Binbusayyis and T. Vaiyapuri, "Comprehensive analysis andrecommendation of feature evaluation measures for intrusion detection," *Heliyon*, vol. 6, no. 7, 2020.

[11] H. Gharaee and H. Hamid, "A new feature selection IDS basedon genetic algorithm and SVM," in *Proc. 8th Int. Symp. on Telecommunications (IST), IEEE*, Tehran, Iran, 2016.

[12] M. A. Ambusaidi, X. He, P. Nanda and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016.

[13] T. Salman, D. Bhamare, A. Erbad, R. Jain and M. Samaka, "Machine learning for anomaly detection and categorization in multi-cloud environments," in *Proc.2017 IEEE 4th Int. Conf. on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, USA, pp. 97–103, 2017.

[14] S. Potluri, S. Ahmed and C. Diedrich, "Convolutional neural networks for multi-class intrusion detection system," in *Proc. Int. Conf. on Mining Intelligence and Knowledge Exploration*, Goa, India, Springer, pp. 225–238, 2018.

[15] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cyber Security*, vol. 4, no. 1, pp. 1–27, 2021.

[16] A. Chauhan, R. Singh and P. Jain, "A literature review: Intrusion detection systems in internet of things," in *Proc. 4th Int. Conf. on Machine Vision and Information Technology (CMVIT)*, Sanya, China, 2020.

[17] H. Alazzam, A. Sharieh and K. E. Sabri, "A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer," *Expert Systems with Applications*, vol. 148, pp. 113249, 2020.

[18] O. Almomani, "A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms," *Symmetry*, vol. 12, no. 6, pp. 1046, 2020.

[19] M. Hammad, W. El-medany and Y. Ismail, "Intrusion detection system using feature selection with clustering and classification machine learning algorithms on the UNSW-NB15 dataset," in *Proc. Int. Conf. on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, Sakheer, Bahrain, pp. 1–6, 2020.

[20] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset," *Journal of Big Data*, vol. 7, no. 1, pp. 1–20, 2020.

[21] C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[22] N. Jacob and M. Yusuf Wanjala, "A review of intrusion detection systems," *Global Journal of Computer Science and Technology, C Software & Data Engineering*, vol. 17, no. 3, 2017.

[23] C. Khammassi and S. Krichen, "A GA-LR wrapper approach for feature selection in network intrusion detection," *Computers & Security*, vol. 70, pp. 255–277, 2017.

[24] T. Mehmod and H. B. M. Rais, "Ant colony optimization and feature selection for intrusion detection," *Proc. Advances in Machine Learning and Signal Processing*, vol. 387, pp. 305–312, 2016.

[25] G. B. Huang, Q. Y. Zhu and C. K. Siew, "Extreme learning machine: A new learning scheme of feedforward neural networks," in *Proc. IEEE Int. Joint Conf. on Neural Networks*, USA, vol. 2, pp. 985–990, 2004.

[26] J. Kennedy and R. C. Eberhart, "Particle swarm optimization," in *Proc. IEEE Int. Conf. on Neural Networks*, Perth, Australia, pp. 1942–1948, 1995.

[27] Y. Y. Chung and N. Wahid, "A hybrid network intrusiondetection system using simplified swarm optimization (SSO)," *Applied Soft Computing* 12(9):3014–3022, 2012.

[28] S. X. Wu and W. Banzhaf, "The use of computational intelligencein intrusion detection systems: A review," *Applied Soft Computing*, vol. 10, no. 1, pp. 1–35, 2010.

[29] L. Dhanabal and S. P. Shantharadah, "A study on NSLKDD dataset for intrusion detection system based on classification algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 446–452, 2015.

[30] S. Revathi and A. Malathi, "Adetailed analysis on NSL-KDD dataset usingvarious machine learning techniques for intrusion detection," *International Journal of Engineering Research & Technology*, vol. 2, no. 12, pp. 1848–1853, 2013.

[31] L. Dhanabal and S. P. Shantharajah, "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 446–452, 2015.

[32] M. A. Ambusaidi, X. He, P. Nanda and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016.

[33] X. Zhang, J. Ran and J. Mi, "An intrusion detection system based on convolutional neural network for imbalanced network traffic," in *Proc. 2019 IEEE 7th Int. Conf. on Computer Science and Network Technology (ICCSNT)*, Dalian, China, pp. 456–460, 2019.

[34] M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish and A. E. Hassanien, "Hybrid intelligent intrusion detection scheme," *Soft Computing in Industrial Applications*, vol. 96, pp. 293–303, 2011.

[35] E. De Hoz, A. Ortiz, J. Ortega and E. De Hoz, "Network anomaly classification by support vector classifiers ensemble and non-linear projection techniques," *Hybrid Artificial Intelligent Systems*, vol. 8073, pp. 103–111, 2013.

[36] M. M. Sakr, M. A. Tawfeeq and A. B. ElSisi, "Filter versus wrapper feature selection for network intrusion detection system," in *Proc. 2019 Ninth Int. Conf. on Intelligent Computing and Information Systems (ICICIS)*, Cairo, Egypt, pp. 209–214, 2019.

[37] P. J. Sajith and G. Nagarajan, "Optimized intrusion detection system using computational intelligent algorithm," in *Proc. Advances in Electronics, Communication and Computing*, pp. 633–639, 2021.

[38] R. Rajendran, P. Kumar, B. Muthukumar and G. Nagarajan, "Hybrid intrusion detection system for private cloud: A systematic approach," *Procedia Computer Science*, vol. 48, pp. 325–329, 2015.