Computer Systems Science & Engineering
DOI:10.32604/csse.2022.021217
Article

Tech Science Press

Hybridized Wrapper Filter Using Deep Neural Network for Intrusion Detection

N. Venkateswaran[1,*] and K. Umadevi[2]

[1]Information and Communication Engineering, Anna University, Chennai, 600025, India
[2]Department of Electronics and Communication Engineering, Sengunthar Engineering College, Tiruchengodu, 637205, India
*Corresponding Author: N. Venkateswaran. Email: nvenkateswaran21@yahoo.com
Received: 27 June 2021; Accepted: 30 July 2021

Abstract: Huge data over the cloud computing and big data are processed over the network. The data may be stored, send, altered and communicated over the network between the source and destination. Once data send by source to destination, before reaching the destination data may be attacked by any intruders over the network. The network has numerous routers and devices to connect to internet. Intruders may attack any were in the network and breaks the original data, secrets. Detection of attack in the network became interesting task for many researchers. There are many intrusion detection feature selection algorithm has been suggested which lags on performance and accuracy. In our article we propose new IDS feature selection algorithm with higher accuracy and performance in detecting the intruders. The combination of wrapper filtering method using Pearson correlation with recursion function is used to eliminate the unwanted features. This feature extraction process clearly extracts the attacked data. Then the deep neural network is used for detecting intruders attack over the data in the network. This hybrid machine learning algorithm in feature extraction process helps to find attacked information using recursive function. Performance of proposed method is compared with existing solution. The traditional feature selection in IDS such as differential equation (DE), Gain ratio (GR), symmetrical uncertainty (SU) and artificial bee colony (ABC) has less accuracy than proposed PCRFE. The experimented results are shown that our proposed PCRFE-CDNN gives 99% of accuracy in IDS feature selection process and 98% in sensitivity.

Keywords: Deep neural network; intrusion detection; machine learning

1 Introduction

Nowadays Computer networks, wireless networks are widely used by variety of applications which are prone to myriad of security threats and attacks. The security challenges that have to be solved originate from the open nature, the flexibility and the mobility of the wireless communication medium [1,2]. In an effort to secure these networks, various preventive and protective mechanisms such as intrusion detection systems (IDS) were developed [3]. Primarily, IDS can be classified as: host based intrusion detection systems (HIDS) and network based intrusion detection systems (NIDS) [4]. Furthermore, both HIDS and NIDS can be categorized into: signature-based IDS, anomaly-based IDS and hybrid IDS [5,6]. An Anomaly

based IDS analyses the network under normal circumstances and flags any deviation as an intrusion. A signature-based IDS relies on a predefined database of known intrusions to pinpoint an intrusion. In this case, a manual update of the database is performed by the system administrators. The associate editor coordinating the review of this manuscript and approving it for publication was Shagufta Henna. In terms of performance, an IDS is considered effective or accurate in detecting intrusions when it concurrently achieves low false alarm rates and high classification accuracy [7]; therefore, decreasing the law false alarm rate as well as increasing the detection accuracy of an IDS should be one of the crucial tasks when designing an IDS. In this paper, the terms wireless intrusion detection system (WIDS) and intrusion detection system (IDS) will be used interchangeably. In order to obtain better network security, a various research were conducted for IDS such as bagged boosting with C5 decision trees [8] and kernel miner [9] which are the earlier detection of IDS. The papers from [10,11] applied Machine learning techniques such as Support vector machine for IDS. The various ML techniques such as Artificial neural network (ANN), SVM and Multivariate adaptive regression spline (MARS) [12–14] were used in IDS to detect the normal traffic from the attacks.

Due to the current network traffic because of processing large amount of data, the security is an issue in IDS [15]. The huge amount of data leads to mathematical difficulties with high computational complexity in classification process. Also these large size of datasets may contains noise, redundancy, and unrelated features which creates challenge to the classification. Processing the large volume of data with all the features will affect the classification accuracy. To address the issues in feature selection methods, this paper proposed a hybrid feature selection called Pearson correlation based Recursive feature elimination to select the relevant features that are close to the data which will increase the classification accuracy. In order to process the large volume of data, the best and well known Deep learning concepts were used in this paper to classify the data. DL has been applied to various fields such as language identification, image processing and pharmaceutical research [16–18]. With this knowledge, the DL technique called Convolutional Deep Neural Network (CDNN) is applied on our work for classification. Our contribution of the paper is as follows,

- This work proposed a hybrid wrapper feature selection method called Pearson Correlation based Recursive Feature Elimination (PCRFE) to remove the redundant and irrelevant features from the dataset. This evaluate the correlation between the features and generate the subset of relevant features using the Recursive Feature elimination technique. Due to the subset of feature selection, this proposed PCRFE-FS technique will improve the detection rate, accuracy of the classification with low computational complexity.
- Convolutional Deep Neural Network (CDNN) is used as a classifier for IDS, Which is the deep learning technique. The efficiency of the proposed technique is evaluated using the performance metrics.
- The experimented results were compared with the previous IDS algorithms in terms of feature selection and previous IDS systems. The evaluated dataset is NSL-KDD dataset.

The rest of the paper is organized as follows: Section 2 outlines the literature related to IDS, Section 3 introduces the proposed feature selection and classification algorithm called PCRFE-CDNN-IDS, Section 4 presents the experimented results and analysis of the comparative study and Section 5 concludes the paper with the future work.

2 Related Work

This section describes about the various literature related to IDS. In order to detect the anomalies in the network traffic of IDS, the IDS dataset called NSL-KDD dataset analyzed in paper. They also analyzed about

the protocols relate to the attacks which is used by the intruders to create the network traffic using the classification algorithms and WEKA tool. They proposed Least square support vector machine based IDS called LSSVM-IS for optimal feature selection. The evaluated datasets are KDD Cup99, NSL-KDD and Kyoto 2006+. Various feature selection algorithms such as Information gain, PCA, Correlation feature selection (CFS), Genetic algorithm, Artificial Bee colony and PSO are analyzed to boost the network IDS.

They concluded that ABC-NIDS performs better than other algorithms. Deep belief network based dimensionality reduction was proposed in paper [19]. They used SVM as classifier and NSL-KDD dataset have been used for analysis. Bi layer behavioral based feature selection was proposed in paper [20] which consists of two layers such as information gain used to rank the features based on the global maxima, a new set of features are selected as 41 to 34 features then in the second layer, the selected features are redacted to find global maximum to reduce the number of features as 34 to 20. The evaluated dataset was NSL-KDD dataset. IDS based on CNN was proposed in paper [21]. To balance the network traffic, before the training of CNN, an algorithm called synthetic minority oversampling technique with edited nearest neighbours (SMOTE-ENN) was applied on the NSL-KDD dataset. This SMOTE-ENN based CNN obtains 83.31% of accuracy.

IDS with deep learning using feed forward deep neural networks (FFDNN) was proposed in paper [22] which is combined with filter based feature selection method. The evaluated dataset was NSL-KDD dataset. Feature selection based on ant colony optimization with two level pheromones applied on KDDCup 99 for IDS [23]. Wrapper based feature selection called Genetic Algorithm (GA) has been applied on IDS in paper [24] and to evaluate the algorithm logistic regression used.

The study on various IDS with bench mark datasets were analyzed in paper [25] to understand the different attacks and relevant issues and problems of IDS. They also evaluated the performance of IDS with machine learning classification algorithms and suggested some feature selection classification algorithm for IDS. They suggested that Auto encoder and Recurrent Neural network of deep learning performs better. And also the combination of SVM with RBMS also performs better. Feature selection algorithm called auto encoder damped with incremental statistics algorithm was proposed in paper [26] and HELAD used as a classifier combined with LSTM which is evaluated MAWLAB dataset.

Principal component analysis and auto encoder used as a feature selection algorithm in paper [27] and CNN as a classifier on KDD Cup 99 dataset. They obtain the accuracy of 94% and 93% of detection rate. The paper [28] evaluated the ten ML algorithm on NSL-KDD dataset for IDS in order to choose the best classifier based on the performance metrics. Convolutional neural network based classification was proposed on paper [29] which obtains high accuracy and FAR rates. Deep stacked auto encoder based feature extraction was proposed in paper [30] and softmax used as a booting for classification on NSL-KDD dataset with the accuracy of 98.6% and UNSW-NB15 dataset with the accuracy of 92.4%. Paper [31] proposed a feature selection approach using information gain used to find the attack on NSL-KDD dataset in order to find the best feature set for each attack based on threshold. The classifiers with Random forest and PART obtains high precision and accuracy. Based on the reviewed literature, IDS with better performance is still needed and based on the knowledge of the reviewed techniques we proposed optimized feature selection with deep learning for IDS.

3 Proposed Pearson Correlation Recursive Feature Elimination Methodology

Deep learning is types of machine learning techniques which are inspired by artificial neural networks algorithms that imitate the way the human brain think rather machine learning used the simpler predictive models. Deep learning concepts require a larger datasets for processing. For smaller volume of data, deep learning is not suited one. Since DL requires large volume of data, the parameters, computation and formulation to train the ANN takes time and the methods to train the models with improved accuracy are

still in research. The repeated and irrelevant features in the dataset are leads a problem in network traffic classification. These irrelevant features will reduce the accuracy of the classification and also make the classification system as slow. In this proposed work, the hybrid version of filter and wrapper based feature selection algorithm with deep learning techniques. This proposed work is evaluated in network intrusion detection. The proposed Intrusion Detection system overview is shown in Fig. 1.

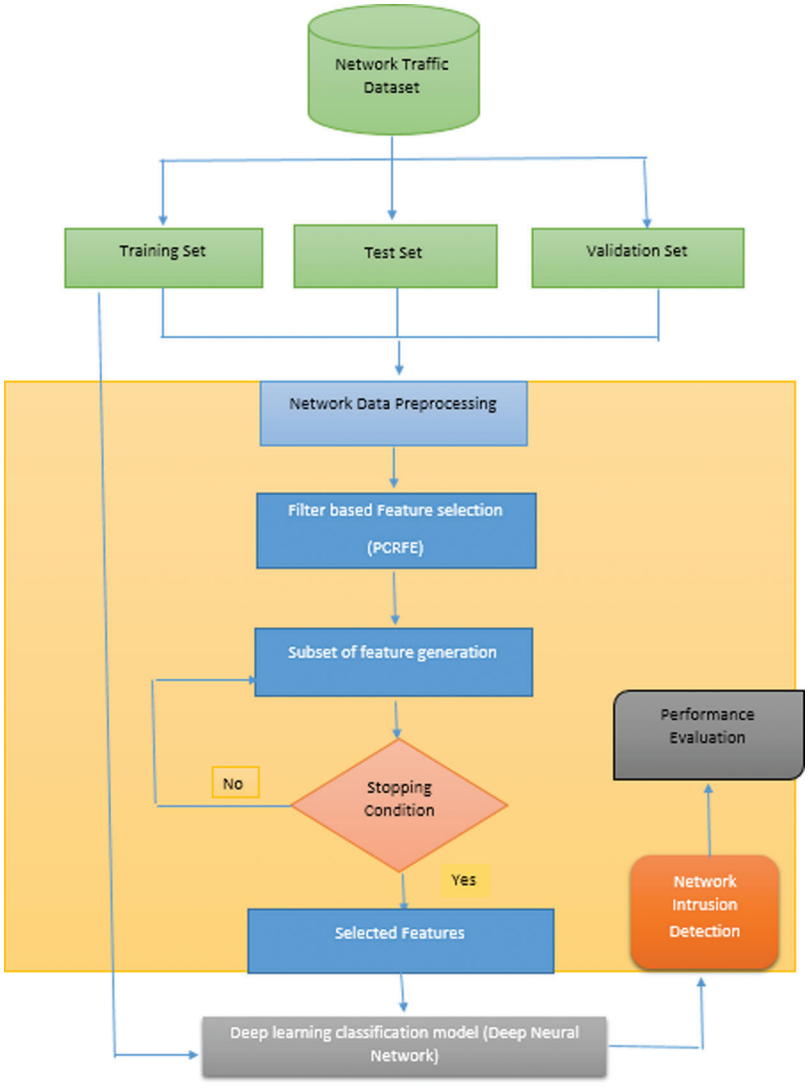

Figure 1: Proposed PCRFE-DNN-IDS architecture

Initially the network data set is divided into three datasets such as training, testing and validation in the ration of 6:2:2. The raw data are preprocessed to remove the missing and redundant features. Then the proposed work uses the filter such as Pearson correlation based recursive feature elimination algorithm for feature selection. Until the stopping condition met, the subset of features are selected using the proposed filter based FS approach. Selected features are then trained and classified using the deep learning algorithm called Deep Neural Network. These proposed PCRFE based DNN classification approach analyzed with the intrusion detection dataset to prove the efficiency of the proposed work.

3.1 Network Data Preprocessing

The preprocessing is important step before proceeding the classification approaches. the raw data is the combination of numeric and non-numeric data. The deep neural network can process numeric data. Using scikit learn in python, all the non-numeric symbols are transformed into numeric value. Normalization is the process to scale the data values into range [0, 1]. To apply the normalization on the data, the minimum value of each feature value is subtracted and divided with the range as (maximum-minimum) using the following Eq. (1)

$$X_{normalized} = \frac{X_i - \min(X_i)}{MAx(X_{i)} - Min(X_i)} \tag{1}$$

where X_i-ith feature, i = 1…. n, n-total number of features.

3.2 PCRFE Based Feature Selection

The normalized data are then given as input to feature engineering part called filter based feature selection. In this proposed work, hybrid FS approach called Pearson correlation based RFE used. Pearson correlation is the relationship between the data that vary between the range [−1, 1]. Value 1 means positive correlation, 0 means no correlation and −1 means negative correlation. This method remove the features at once from the machine learning model rather than removing the features at each step. Because of this, it is a faster than wrapper based filters and embedded filter methods. And also this method uses a threshold value to rank the features. Minimum the threshold will remove more features. So choosing the threshold value is next important choice. Based on corresponding value of correlation coefficient threshold is chosen. Here, threshold is defined based on testing the multiple hypotheses also.

Algorithm:

Input: Normalized Feature set

Output: Selected Feature subset

Step 1: for all features i = 1…n

Step 2: Compute the correlation coefficient of the feature using the Eq. (2)

$$PC_{xiyi} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{2}$$

Step 3: Eliminate the features using the PCRFE Eq. (3),

$$PCRFE(x_i) = \sum_{i=1}^{n}\left(y_{ij} - \sum_{j=1}^{d} PC_{x_i y_j} \times x_i\right)^2 \tag{3}$$

Step 4: if ($PCRFE(x_i) \geq threshold$ then

Step 5: Add the features into the subset

Step 6: end if

Step 7: repeat step 2 to 6 till all the features evaluated

Step 8: end for

The normalized and selected features are then fed into convolutional deep neural network (CDNN) for classification.

3.3 Convolutional Deep Neural Network

In this proposed work, CDNN is used as a deep learning method for IDS to classify the normal and abnormal data in the network traffic. In most cases of CNN uses the image as input while the grey images with 2D and color images with 3D representation. Our evaluation of proposed work consider the NSL-KDD data set. Among the 121 features of the dataset, the selected features are then transformed into 11×11 array. In the proposed DNN, there are five layers are involved. Convolutional, pooling, input layer, hidden layer an output layer which are fully connected. The convolution and pooling layer are operate the activation functions. The data are transformed form input layer to class layer through hidden layer. This deep neural network used sigmoid activation function for binary classification and Softmax activation function for multi class classification. The proposed CDNN-IDS is shown in Fig. 2. The input 11×11 dimension array is given as input to the input layer. The convolution layer contains multiple kernel values which is related to bias and weights. Convolution process is done using the Eq. (4).

$$C_{x_i,y_i} = \sum_{i=1}^{p*q} w_i v_i \tag{4}$$

where kernel k = p*q size, w_i –weight and v_i = image luminance value of the image dimension x_i, y_i. After the convloution, the dimension reduced into the size of 2×2 as pooling stage. Between the input and hidden layer the bias value b is added and the activation function is h.

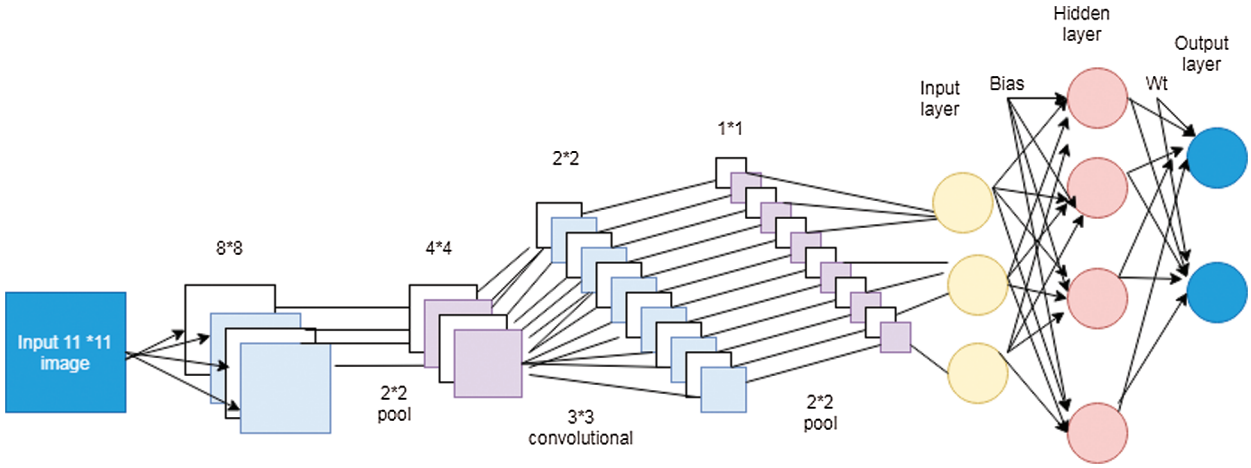

Figure 2: Proposed CDNN-IDS architecture

In this work for binary classification sigmoid function used as activation function and multi class classification softmax activation function used as Eq. (5). In this work, four hidden layers are used.

$$sigmoid\ h = \frac{1}{1 + e^{-x_i}} \qquad softmax(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{n} e^{x_j}} \tag{5}$$

The hidden layers takes inputs from input layer and performed the activation operation and then produces the output based on the weight value. The computation of the hidden layer with non linear loss function is declared as Eq. (6)

$$z_{x,y} = h\sum_{i=1}^{k} w_i v_i \tag{6}$$

where h is the activation function. The loss value of the actual and predicted value is calculated using the Eq. (7). The minimization of the loss functions will leads to get better result in deep learning neural network.

$$loss(input_n, output_n) = \frac{1}{n}\sum\nolimits_{i=1}^{n}(output_i, f(input_i)) \tag{7}$$

The proposed Network Intrusion Detection using filter based deep learning is shown in Fig. 3. The input data are pass on to various level of processing called normalization, feature elimination and classification using the proposed approaches.

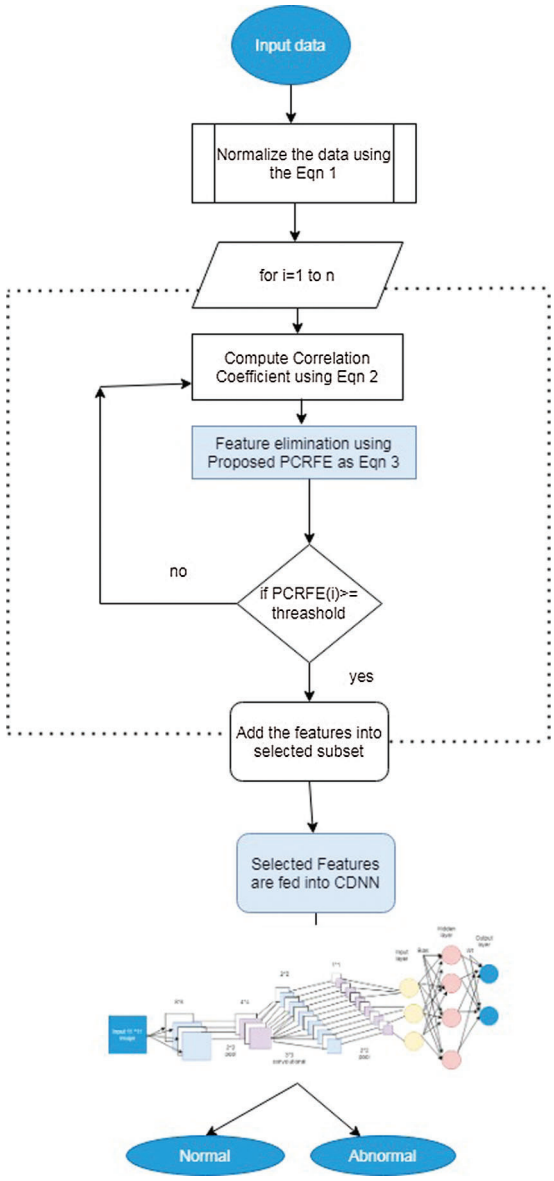

Figure 3: Proposed PCRFE-CDNN- IDS workflow

4 Results and Discussions

The proposed work has been experimented as a binary classification on NSL-KDD dataset. This proposed model is implemented using python and python deep learning library called keras. This CDNN-IDS consist of two convolution, two pooling and three fully connected layers of input, hidden and output is used. The pool size is declared as 2\ast 2. For the three fully connected layers two neurons are used to train the model. The dropout rate of this model is 0.3. The proposed work is evaluated using the performance metrics.

4.1 Data Set

To analyze the performance of the proposed PCRFE-CDNN-IDS system, the benchmark network traffic dataset called NSL-KDD used. It is proven to be the best dataset for testing the IDS. There are 41 features that are divided as basic, conent based and time based attributes. Training set consist of 22 attacks and 16 attacks are considered as testing set. The attacks are categorized as 1) Denial of Service attacks (DoS) 2) Probe Attacks (PA) 3) Remote to Local attacks (R2L) and 4) User to Root attacks (U2R). The IDS attacks with detailed explanation and the training, testing data are mentioned in Tab. 1. with the binary class.

Table 1: NSL-KDD attacks and training, testing data

Class	Attack	Description	NSL-KDD dataset	
			Training data	Testing data
Normal	No attack	Connection as normal	67343	9710
Abnormal	DoS	Attackers make the network resources as down. Make the system with traffic. ex. Network bandwidth. This attack violates the data availability	45927	7458
	Probe	Obtain the detailed specification of network configuration details. Intruders trying to collect the target machine informationss. This attack violates the system confidentiality and integrity.	11656	2422
	R2L	Illegal access. Intruders make traffic flow and get unauthorized access. This violates system integrity.	995	2887
	U2R	Obtain the root of the PC. This also violates the integrity of the system.	52	67

4.2 Features Selection

Among the 41 features of NSL-KDD dataset, the proposed feature selection approach called Pearson Correlation based Recursive Feature Elimination, eliminate the irrelevant features from the features set recursively and add the selected features to feature subset. This proposed filter based feature selection select 4 relevant attributes for further processing. To evaluate the performance of the proposed Feature Selection algorithm, number of selected features of different FS algorithms are compared with the proposed filter based FS approach which is represented in Tab. 2. The selected features name by the proposed model is represented in Tab. 3.

Table 2: Feature selection approaches with selected features

FS approaches	No of features	Selected features
All features	41	f1, f2, f3, f4, f5, f6.f7, f8, f9, f10, f11, f12, f13, f14, f15, f16, f17, f18, f19, f20, f21, f22, f23, f24, f25, f26, f27, f28, f29, f30, f31, f32, f33, f34, f35, f36, f37, f38, f39, f40, f41
FMIFS [2]	18	f5, f30, f6, f3, f4, f29, f12, f33, f26, f37, f39, f34, f25, f38, f23, f35, f36, f28
FLCFS [2]	22	f29, f12, f33, f39, f4, f23, f34, f25, f26, f38, f8, f35, f19, f32, f18, f3, f6, f40, f30, f5, f27, f22
Proposed PCRFE	6	f3, f5, f30, f4, f6, f29

Table 3: Selected feature name by PCRFE

Selected feature	Feature name
F3	Service
F5	Src_bytes
F29	Diff_srv_rate
F3	Flag
F6	Dst_bytes
F29	Same_srv_rate

4.3 Evaluation Using Performance Metrics

The proposed PCRFE-CDNN-IDS system is compared with the existing approaches to analyze the performance using the performance metrics such as Accuracy, False positive rate (FPR), False negative rate (FNR), Sensitivity/True positive rate (TPR), Specificity/True negative rate (TNR) and recall/Attack Detection rate (ADR) [3]. The evaluation metrics equations are represented as

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

$$FPR = \frac{FP}{FP + TN} \tag{9}$$

$$FNR = \frac{FN}{FN + TP} \tag{10}$$

$$SN = \frac{TP}{TP + FN} \tag{11}$$

$$SP = \frac{TN}{TN + FP} \tag{12}$$

$$ADR = \frac{TP}{TP + FN} \tag{13}$$

4.4 Proposed System Evaluatin Interms of Feature Selection

The proposd work is evaluated with the total number of features and the selected fatures using proposed PCRFE feature selection. The evalurated resutls are shown in Tab. 4.

Table 4: Performance evaulation of proposed work with feature subset

Features	ACC	FPR	FNR	SN	SP	ADR
41	0.91	0.04	0.154	0.82	0.98	0.84
6	0.99	0.014	0.25	0.97	0.98	0.98

From the table, the accuracy of 99% is obtained while reducing feature set. The propsoed CDNN-IDS with all the features are evaluated first which obtain the accuracy of 91%. While using the propsoed Feature selecton scheme called PCRFE, the accuracy percentage of the classification is improved by 8% and obtain 99% of accuracy on classificaiton of the IDS data using the propsoed Feature selection and deep learning model. This evaluation is illustrated in Fig. 4.

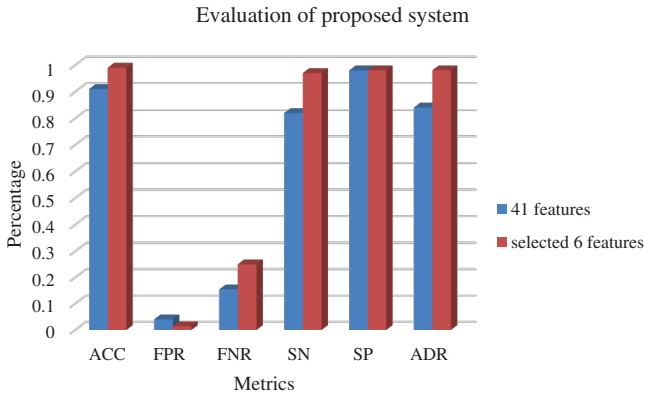

Figure 4: Evaluation of proposed PCRFE + CDNN-IDS

The proposed work feature selection performance is compared with the existing FS on IDS such as, Discrete differential equation [4], Gain ratio [5], symmetrical uncertainty [6] and ABC [3]. The experimented results are shown in Tab. 5 and illustrated in Fig. 5. From the evaluated results, our proposed pearson correlation based recursive feature elimination reduce the feature set into 6. Which is the most relevant features for classification and obtained high accuracy of 99% compared to other existing IDS feature selection schemes. Hence, the feature selection we proposed will reduce the feature set and select the relevant features which guarantee the accuracy of the IDS system.

4.5 Performance Comparison of Proposed with Existing IDS Systems

In order to prove the deep neural network based IDS systems, our proposed convolutional deep neural network based IDS is compared with the existing IDS systems such as DMNB [7], DBN-SVM [19], Bi-layer behavioral-based [20], TUIDS [32], FVBRM [33], PSOM [34] and LSSVM-IDS + FMIFS [2]. The experimented results is represented in Tab. 6. The accuracy and FPR is illustrated in Figs. 6 and 7. From the experimented results of the proposed work, its proven that our proposed filter based feature selection with deep learning IDS obtain high classification accuracy of 99.96% with the minimum False positive rate of 0.23. Hence the proposed IDS achieves high accuracy than others with low FPR than others.

Table 5: Evaluation based on IDS feature selection

Metrics	Feature selection approaches				
	DDE	GR	SU	ABC	Proposed PCEFE
Selected features	16	35	32	22	**6**
ACC	88.6	84.34	85.05	96.76	**99.34**
SN	89.73	86.13	84.92	97	**98.9**
SP	88.33	87.58	87.43	96.7	**97.95**
ADR	91.23	88.01	86.34	97.56	**98.76**

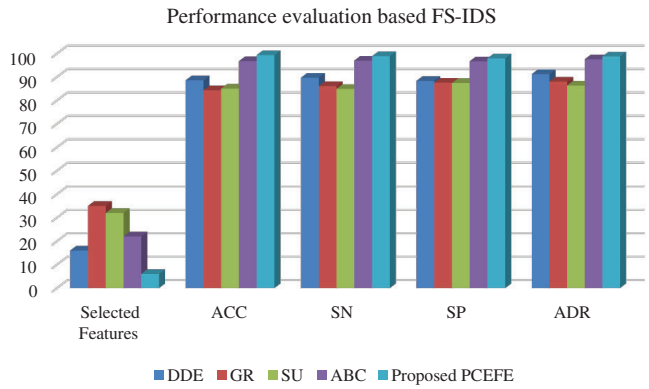

Figure 5: Illustration of different IDS feature selection with proposed FS

Table 6: Performance evaluation of various IDS with Proposed PCRFE + CDNN-IDS

IDS systems	Features	Accuracy	FPR
DMNB	41	96.53	1.76
DBN-SVM	41	92.53	2.43
Bi-layer behavioral-based	20	97.24	3.5
TUIDS	41	94.32	2.3
FVBRM	24	93.23	2.7
PSOM	10	95.87	3.1
LSSVM-IDS + FMIFS	18	98.6	1.02
proposed PCRFE + CDNN-IDS	**6**	**99.96**	**0.23**

Hence the experimented result with NSL-KDD dataset of the proposed pearson correlation based recursive feature elimination reduces the irrelevant features in a secure way which leads to increase the accuracy level. Our proposed convolutional deep neural network classify all four Network attacks of DoS, Probe, R2L and U2R with high accuracy. It is proven that our proposed deep learning approach obtain better result on intrusion detection system.

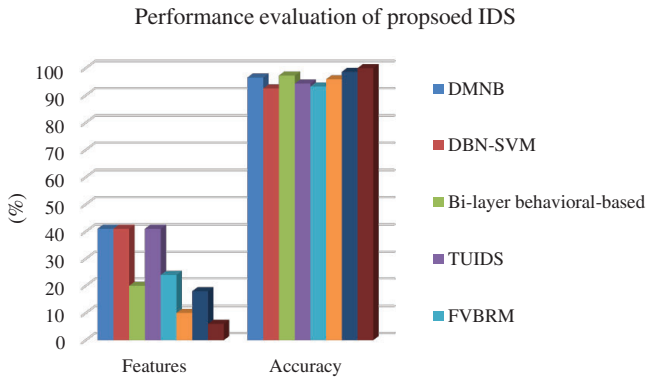

Figure 6: Illustration of the performance of proposed IDS

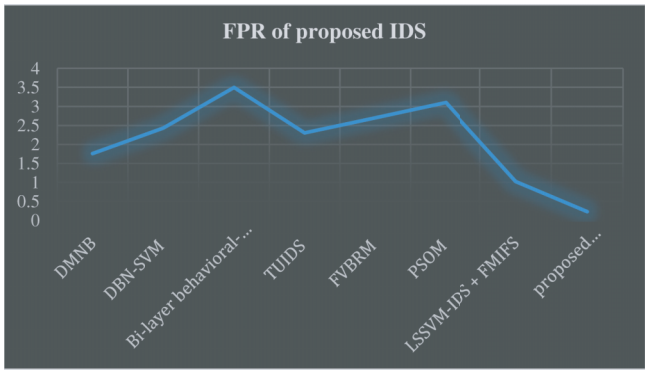

Figure 7: FPR of proposed IDS

5 Conclusion

In this paper, we proposed Pearson correlation based recursive feature elimination (PCRFE) for reducing the redundancy among the features using recursive feature elimination and create the relevant subset of features that are correlated. The selected subset feature data are then classified using the DL method called CDNN for better detection of intruders. The evaluation is done using NSL-KDD dataset. Based on the experimented results, the proposed PCRFE-CDNN-IDS obtains better performance in detecting intrusions among the network. The comparative analysis with various IDS can also prove that our proposed IDS is efficient. In future, the proposed IDS will apply for multi class classification to improve the detection rate with optimized feature selection strategies and will try with some other IDS datasets other than NSL-KDD to know the efficiency of the proposed scheme.

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

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Dhanabal and S. 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.

[2] 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.

[3] M. M. Sakr, M. A. Tawfeeq and A. B. ElSisi, "Filter versus wrapper feature selection for network intrusion detection system," in *Proc. ICICIS*, Cairo, Egypt, pp. 209–214, 2019.

[4] N. T. Pham, E. Foo, S. Suriadi, H. Jeffrey and H. F. M. Lahza, "Improving performance of intrusion detection system using ensemble methods and feature selection," in *Proc. ACSW*, Queensland, Australia, pp. 1–6, 2018.

[5] N. K. Kanakarajan and K. Muniasamy, "Improving the accuracy of intrusion detection using gar-forest with feature selection," in *Proc. FICTA*, Durgapur, India, pp. 539–547, 2016.

[6] Z. Markov and I. Russell, "An introduction to the WEKA data mining system," *ACM SIGCSE Bulletin*, vol. 38, no. 3, pp. 367–368, 2006.

[7] M. Panda, A. Abraham and M. R. Patra, "Discriminative multinomial naive Bayes for network intrusion detection," in *Proc. IAS*, Atlanta, GA, USA, pp. 5–10, 2010.

[8] B. Pfahringer, "Winning the KDD99 classification cup: Bagged boosting," *ACM SIGKDD Explorations Newsletter*, vol. 1, no. 2, pp. 65–66, 2000.

[9] I. Levin, "KDD-99 classifier learning contest LL soft's results overview," *ACM SIGKDD Explorations Newsletter*, vol. 1, no. 2, pp. 67–75, 2000.

[10] D. S. Kim and J. S. Park, "Network-based intrusion detection with support vector machines," in *Proc. ICOIN*, Jeju Island, Korea, pp. 747–756, 2003.

[11] A. Chandrasekhar and K. Raghuveer, "An effective technique for intrusion detection using neuro-fuzzy and radial svm classifier," in *Proc. in Computer Networks & Communications (NetCom)*, Toronto Canada, pp. 499–507, 2013.

[12] S. Mukkamala, A. H. Sung and A. Abraham, "Intrusion detection using an ensemble of intelligent paradigms," *Journal of Network and Computer Applications*, vol. 28, no. 2, pp. 167–182, 2005.

[13] S. Maheswaran, S. Sathesh, Gayathri, E. D. Bhaarathei and D. Kavin, "Design and development of chemical free green embedded weeder for row based crops," *Journal of Green Engineering*, vol. 10, no. 5, pp. 2103–2120, 2020.

[14] S. Sathesh, V. A. Pradheep, S. Maheswaran, P. Premkumar, N. S. Gokul *et al.*, "Computer vision based real time tracking system to identify overtaking vehicles for safety precaution using single board computer," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 7, pp. 1551–1561, 2020.

[15] M. A. Ambusaidi, X. He and P. Nanda, "Unsupervised feature selection method for intrusion detection system," in *Proc. Trustcom*, Helsinki, Finland, vol. 1, pp. 295–301, 2015.

[16] I. LopezMoreno, J. GonzalezDominguez, D. Martinez, O. Plchot, J. Gonzalez-Rodriguez *et al.*, "On the use of deep feedforward neural networks for automatic language identification," *Computer Speech & Language*, vol. 40, pp. 46–59, 2016.

[17] K. He, X. Zhang, S. Ren and J. Sun, "Delving deep into rectifiers: surpassing human-level performance on imagenet classification," in *Proc. ICCV*, Santiago, Chile, pp. 1026–1034, 2015.

[18] S. AgatonovicKustrin and R. Beresford, "Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research," *Journal of Pharmaceutical and Biomedical Analysis*, vol. 22, no. 5, pp. 717–727, 2000.

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

[20] H. F. Eid, M. A. Salama, A. E. Hassanien and T. H. Kim, "Bi-layer behavioral-based feature selection approach for network intrusion classification," in *Proc. FGIT*, Jeju Island, Korea, pp. 195–203, 2011.

[21] X. Zhang, J. Ran and J. Mi, "An intrusion detection system based on convolutional neural network for imbalanced network traffic," in *Proc. ICCSNT*, Dalian, China, pp. 456–460, 2019.

[22] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019.

[23] T. Mehmod and H. B. M. Rais, "Ant colony optimization and feature selection for intrusion detection," in *Proc. MALSIP*, Ho Chi Min City, Vietnam, pp. 305–312, 2016.

[24] 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.

[25] C. Kalimuthan and J. A. Renjit, "Review on intrusion detection using feature selection with machine learning techniques," *Materials Today: Proceedings*, vol. 33, pp. 3794–3802, 2020.

[26] Y. Zhong, W. Chen, Z. Wang, Y. Chen, K. Wang *et al.*, "HELAD: A novel network anomaly detection model based on heterogeneous ensemble learning," *Computer Networks*, vol. 169, pp. 107049, 2020.

[27] Y. Xiao, C. Xing, T. Zhang and Z. Zhao, "An intrusion detection model based on feature reduction and convolutional neural networks," *IEEE Access*, vol. 7, pp. 42210–42219, 2019.

[28] H. Malhotra and P. Sharma, "Intrusion detection using machine learning and feature selection," *International Journal of Computer Network & Information Security*, vol. 11, no. 4, pp. 3794–3802, 2019.

[29] K. Wu, Z. Chen and W. Li, "A novel intrusion detection model for a massive network using convolutional neural networks," *IEEE Access*, vol. 6, pp. 50850–50859, 2018.

[30] F. A. Khan, A. Gumaei, A. Derhab and A. Hussain, "A novel two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[31] M. Abdullah, A. Alshannaq, A. Balamash and S. Almabdy, "Enhanced intrusion detection system using feature selection method and ensemble learning algorithms," *International Journal of Computer Science and Information Security*, vol. 16, no. 2, pp. 48–55, 2018.

[32] P. Gogoi, M. H. Bhuyan, D. Bhattacharyya and J. K. Kalita, "Packet and flow based network intrusion dataset," in *Proc. IC3*, Noida, India, pp. 322–334, 2012.

[33] S. Mukherjee and N. Sharma, "Intrusion detection using naive Bayes classifier with feature reduction," *Procedia Technology*, vol. 4, pp. 119–128, 2012.

[34] E. De La Hoz, A. Ortiz, J. Ortega and E. De la Hoz, "Network anomaly classification by support vector classifiers ensemble and non-linear projection techniques," in *Proc. HAIS*, Salamanca, Spain, pp. 103–111, 2013.