IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 3, Ser. IV (May - June 2019), PP 47-55
www.iosrjournals.org

A Hybrid Feature Extraction Method for Network Intrusion Detection System

K.NandhaKumar[1], Dr.S.Sukumaran [2]
[1](Ph.D Scholar, Department of Computer Science Erode Arts and Science College, Erode, Tamilnadu, India)
[2](Associate Professor, Department of Computer Science, Erode Arts and Science College, Erode, Tamilnadu, India)
Corresponding Author: K.NandhaKumar

Abstract: *Intrusion Detection System (IDS) is one of the important and useful technologies that used to monitor systems or networks. Several researchers have performed feature extraction methods to improve the performance of IDS for detecting network traffic and malicious attacks. Different input features will change the detection performance dramatically when using IDS. The classification process could be prolonged when using high-dimensional features in a large number of network traffic. Recently, feature representation and application of several classifiers became a keen interest for researchers to develop a new strategy to improve the classification performance. In this paper, a hybrid feature extraction (SA_PCA) is proposed from the combination of two algorithms namely Sparse Auto-encoder (SA) and Principal Component Analysis (PCA) for extracting high-level feature description to low-level features. Then, the extracted features are used for the classification using different classifiers. The hybrid SA_PCA is compared with other existing extraction methods that proposed by previous researchers. The simulation results for the proposed method includes: SA_PCA used to extract low-level feature from high-dimensional features and compared with other works and the extracted feature set is used for classification process using existing classifiers. The results show that the proposed hybrid method is more efficient for IDS.*

Keywords: *Feature Extraction, Intrusion Detection System (IDS), Machine Learning, Principal Component Analysis (PCA), Sparse Auto-encoder (SA).*

Date of Submission: 01-06-2019 Date of acceptance: 17-06-2019

I. Introduction

The situation for the network security becomes more complicated with the development of new Internet technologies like mobile payment, file sharing, and instant messaging. Moreover, the security environment of the network is threatened seriously by the attackers who become more invisible and cost of the attack is reduced further. Intrusion detection system (IDS) is an influential defense technology that has grown rapidly and become one of the key technologies for ensuring security aspects in network system. The IDS is developed for the network security to control its protection system which helps in monitoring network-systems operations that based on the security strategy and different intrusion behavior like result or attempt are found that automatically respond to prevent intrusion or illegal access effectively [1]. Two types of processing methods are included by IDS and these are anomaly-detection and misuse-detection. The intrusion behavior model is defined accurately in advance by the misuse-detection system. If the exact pattern of the attacker's attacks match with pattern-library in the detection system then the intrusion behavior is detected. The consideration of intrusion activity for anomaly detection system is unknown which is a subset of unusual activity. The invasion event is considered when normal behavior pattern is deviated for a certain extent [2] [3].

Many researchers have used machine learning classifiers for improving efficiency and performance for the intrusion detection system and the breakthrough progress are achieved. Moreover, only satisfactory results are obtained from most of the machine learning classifiers in small datasets. Space complexity and time complexity are the two main limitations that usually faced by these algorithms when they are used for large-scale IDS. The main reasons for this kind of situation are due to the input data that has attributes with nonlinear characteristics and high dimension. Therefore, dimension reduction of input data is an essential step for the process of intrusion detection that should be more effective on high dimensional data.

In 2006, an article is published by a professor named Hinton working in University of Toronto in Canada on deep learning in science. In his research, the artificial intelligence and big data are analyzed that set of a waving research. Also, many hidden layers are present in the deep artificial neural networks (DANN) that has tremendous capability of learning features and this result facilitate the original data in the form visualization and performance classification. Furthermore, huge workload is reduced by DANN technique for the feature

extraction process and the efficiency is improved. Deep learning and principal component analysis are one of the best solutions for the intrusion detection system due to the outstanding performance that deals with complex and large scale data. Hence, stack auto-encoder (SAE) with principal component analysis model is proposed for the dimension reduction of IDS samples. Furthermore, we use the extracted features for classification process using machine learning classifiers and compared the results with other existing methods [4].

In the following segments, Section II discuss the related works presented by several researchers for intrusion detection system using deep learning and machine learning techniques, Section III describes the proposed methodology of the hybrid feature extraction method and description of the dataset, Section IV describes the proposed work process, Section V discuss the results obtained from the overall proposed work and comparison with other existing models, Section VI concludes the work with some future enhancements.

II. Related Works

In [5] discussed the state of the art survey regarding applications of deep learning within health monitoring machine. The conventional machine learning techniques are compared experimentally with four common deep learning methods and these are Restricted Boltzmann Machine (RBM), auto-encoders, Recurrent Neural Network (RNN), and Convolutional Neural Network (CNN). From his survey, it is concluded that better accuracy is given by deep learning techniques than that of conventional methods. Alrawashdeh and Purdy [6] performed unsupervised feature depletion by using RBM which have only one hidden layer. ADBN is produced by passing weights to another RBM. Logistic Regression classifier that is trained with 10 epochs is present in fine tuning layer in which pre-trained weights are passed. The KDD Cup 99 dataset is used for the evaluation using the proposed technique. The simulation results shows 97.90% of detection rate is obtained with 2.47% of false negative rate.

Kim et al. [7] analyzed targeted persistent threats that are much advanced. 100 hidden units were used to propose Deep Neural Network (DNN) which combined with ADAM optimizer and activation function named Rectified Linear Unit. In his research, Potluri and Diedrich [8] presented a technique in which 3 hidden layers are present in DNN that uses 41 features. Hence, 1 s0ft-max and 2 auto-encoders are used for the proposed method. Fewer classes extracted give more accurate when using more classes. A. Javaid et al. [9] built a flexible and effective NIDS using a deep learning based approach that referred to as Self-Taught Learning (STL) that used to combine soft-max regression and sparse auto-encoder. NSL-KDD dataset is used for the evaluation process and implemented the solution. The classification accuracy levels are claimed by the authors in both 5-class and binary classification. The f-score obtained an average of 75.76% for their 5-class classification. Cordero et al. [10] learned normal network flows by proposing an unsupervised method. Here, the concepts of deep learning like dropout, auto-encoder, and RNN are used. The evaluation of the proposed method for the exact accuracy is not revealed fully.

You et al. [11] presented an auditing tool based on automatic security for short messages (SMS) by using RNN model. The evaluation result of this research shows that 92.7% accuracy rate is obtained than that of Naïve Bayes and SVM. Wang et al. [12] detected malicious JavaScript by using 3 layers SDA with linear regression. The evaluation process done against other methods that it has highest positive rate and best FPR. N. SenthilMurgan and G. Usha Devi [13] presented a hybrid feature extraction model using the combination of principal component analysis and linear regression for extracting reliable features from large dataset and obtained the high performance rate using machine learning classifiers. Also in paper [14], the features extracted by the proposed model used for classification process of another hybrid model that includes ML algorithms and Evolutionary algorithms and the results for this research for large dataset given higher when compared with other classifiers.

Brauckhoff et al. [15] analyzed the implementation with KL expansion and PCA for anomaly detection. In his research, the right number of PC is issued for the analysis. Ringberg et al. [16] discussed the PCAs sensitivity for anomaly detection, impact of anomaly size, issues related to number of PC and compressive study has given for the issues related to Geant and Abilene networks. Also, G. Wang et al. [17] presented a new approach using fuzzy clustering and artificial neural network for intrusion detection. Here, low-detection rate of low frequency attack problems are solved by this proposed technique and higher detection rate is achieved. Bamakan et al. [18] presented particle swarm optimization based on time-varying chaos into intrusion detection system that used to select the parameters of Support Vector Machine (SVM) that has some characteristics of low false alarm rate and high detection rate. Ambusaidi et al. [19] used least square SVM with the feature selection that are combined mutual information selection that makes less computational cost and speed in the detection of features. Osanaiye et al. [20] achieved an optimal solution by combining four filter methods output into an feature selection method based on ensemble multi filter that gives a high performance in detecting DDOS.

Arman Tajbakhsh et al. [21] used Fuzzy association rules for the proposed classification algorithm for building classifiers. Compatibility threshold is used for exploiting rule sets as descriptive models for different classes. In this system, fuzzy membership is defined by using WFCM clustering algorithm for this functions and

feature reduction is done by its hyper edges. Therefore, this paper focus on feature reduction of large dataset by using proposed hybrid method named SA_PCA and analyzes the performance using ML classifiers.

III. Methodology

A. Auto-Encoder

This auto-encoder (AE) is the formation of three-layered unsupervised neural network model that consist of output-layer that known to be reconstruction layer, hidden-layer, and input-layer. Figure 1 shows the basic structure of AE. Figure 2 shows the representation of AE [22].

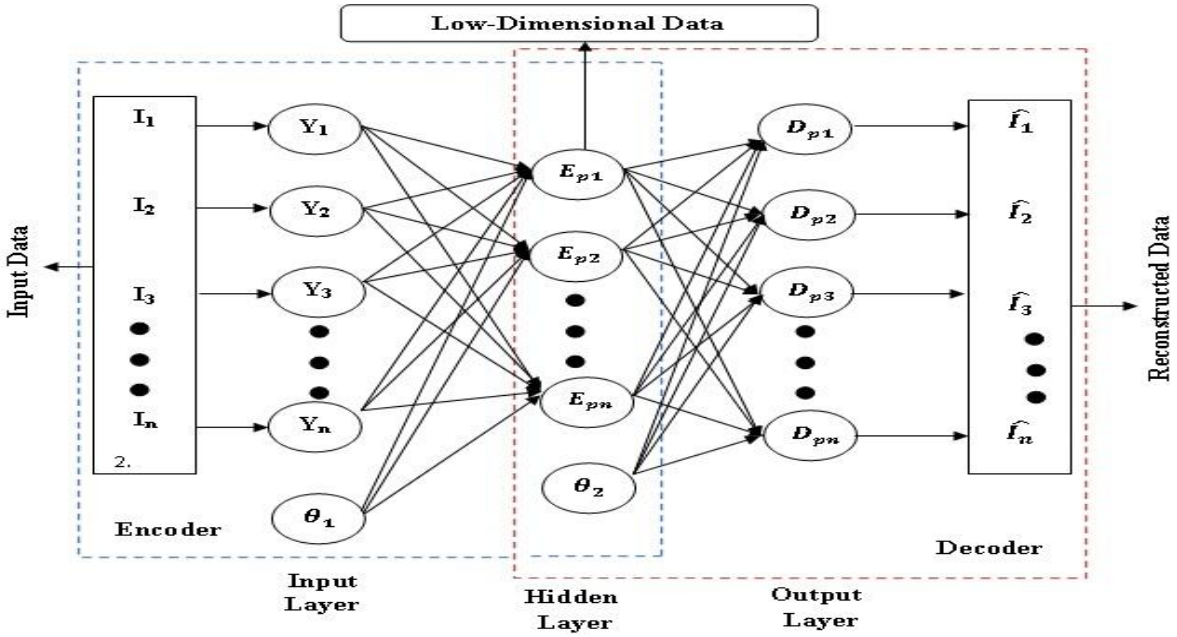

Fig. 1 Basic Structure of Auto-Encoder

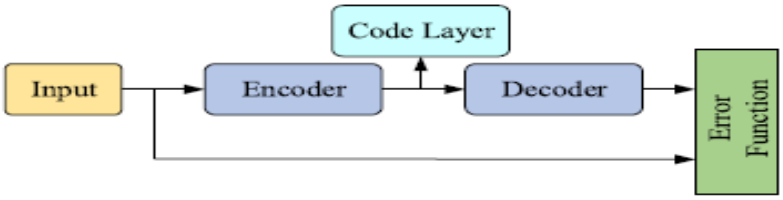

Fig. 2 Representation of Auto-Encoder

Specific feature vectors are transformed gradually by AE into abstract feature-vectors. It can realize well about the non-linear transformation from high-dimensional data space to low-dimensional [23]. There are two stages mainly considered in the processing of automatic encoder and these are Encoding and Decoding and it can be defined as:

The process of encoding from input-layer to the hidden-layer is given by:

$$E_p = d_{\varphi_1}(Y) = \delta(Q_{ij}Y + \theta_1) \tag{1}$$

The process of decoding from the hidden-layer to reconstruction layer is defined by:

$$D_p = d_{\varphi_2}(E_p) = \delta(Q_{ij}E_p + \theta_2) \tag{2}$$

Therefore, from the given formulas denotes that $Y = (y_1, y_2, \dots\dots, y_n)$ is the input data vector and reconstruction vector is denoted by $D_p = (d_{p1}, d_{p2}, \dots\dots, d_{pn})$ for the input-data and low-dimensional vector is given as $E_p = (e_{p1}, e_{p2}, \dots\dots, e_{pn})$ for the hidden-layer.

B. Sparse Auto-Encoder with Principal Component Analysis (SA_PCA)

Figure 3 shows the hybrid combination of Sparse Auto-encoder and PCA in which SA uses the concept of neural network that composed of multiple sparse which connected end-to-end, and PCA is another dimensional reduction technique that works with the principal components of the features [24].

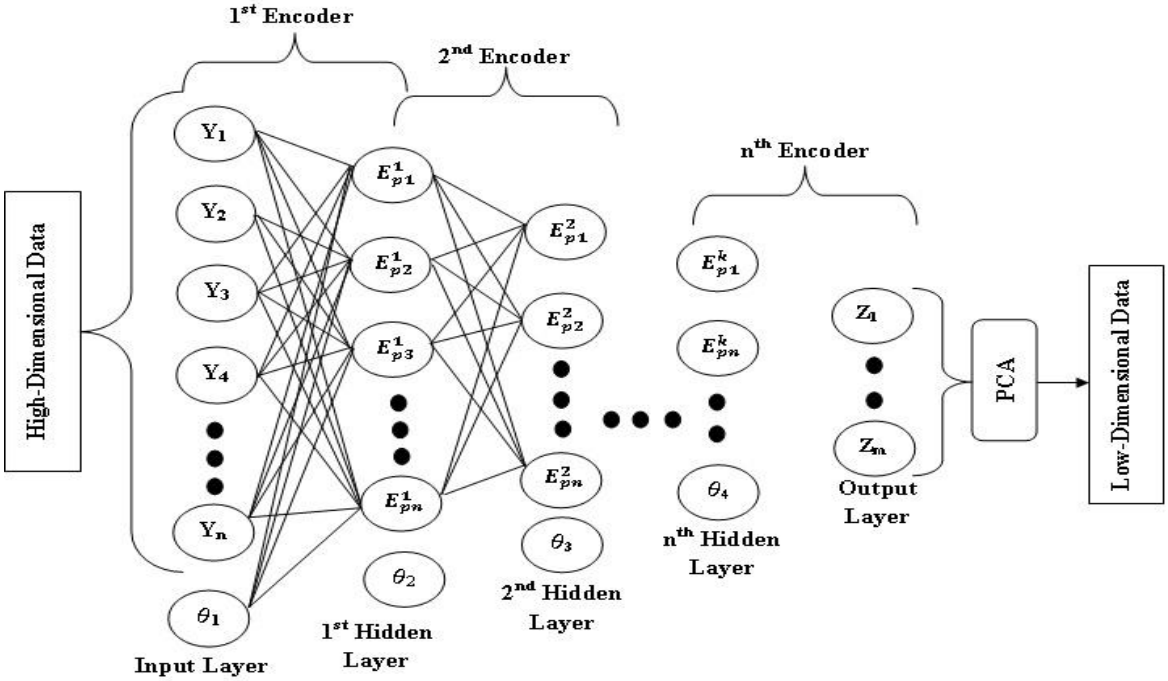

Fig. 3 Structure of SA_PCA

Each layer of SA is sequentially trained by using greedy layer pre-training technique for accessing optimized connection weights and entire bias values of stack auto-encoder network. The error function result between the input-data and output-data is fine tuned using error back propagation method and satisfy the expected requirements.

For error function is denoted by $R_{stack}(K, a)$ and is defined by:

$$\frac{\rho}{\rho k_{ij}^r} V_{sparse}(K, a) = \frac{1}{2n_r} \sum_{r=1}^{n_r} \frac{\rho}{\rho k_{ij}^r} V_{sparse}(K, a, Y(n),) + \gamma k_{ij}^r \quad (3)$$

$$\frac{\rho}{\rho g^r} V_{sparse}(K, a) = \frac{1}{2n_r} \sum_{r=1}^{n_r} \frac{\rho}{\rho g^r} V_{sparse}\left(K, a, Y(n), D_p(n)\right) \quad (4)$$

Therefore, the processing update for bias and weights are given as:

$$k_{ij}^r = k_{ij}^r - \eta \frac{\rho}{\rho k_{ij}^r} V D_p(n)(K, a) \quad (5)$$

$$g^r = g^r - \eta \frac{\rho}{\rho g^r} V(K, a) \quad (6)$$

Where, $Y(n)\ and\ D_p(n)$ is represented as the n[th] original vector and its reconstruction-vector. The update learning rate is indicated by η.

Henceforth, principal component analysis is defined as:

$$\text{PCA } (q, \frac{\rho}{\rho g^r} V_{sparse}(K,a)) \quad (7)$$

$$PC_j = a_1\left(\frac{\rho}{\rho g^r}V_{sparse}(K,a)\right)_2 + a_2\left(\frac{\rho}{\rho g^r}V_{sparse}(K,a)\right)_2 + \ldots\ldots + a_m\left(\frac{\rho}{\rho g^r}V_{sparse}(K,a)\right)_m \quad (8)$$

Where,

PC_j - is the principal component of 'j',

$\frac{\rho}{\rho g^r}V_{sparse}(K,a)$ - is the extracted feature,

a_m – Numerical coefficient $\frac{\rho}{\rho g^r}V_{sparse}(K,a)$,

q – Dimension space,

IV. Proposed Work

A. Framework

Figure 4 shows the framework of the proposed SA_PCA model and its workflow. In this framework, the original dataset is preprocessed for removing null values that can be used for testing and training process. Further, the dataset after preprocessing is separated into two parts: a training-set and a testing-set. Here, pre-training and fine-tuning is done by using training-set and the testing-set is used as the input for the proposed model and finally performance of the machine learning classifiers is analyzed and the effectiveness of the proposed SA_PCA is validated [25].

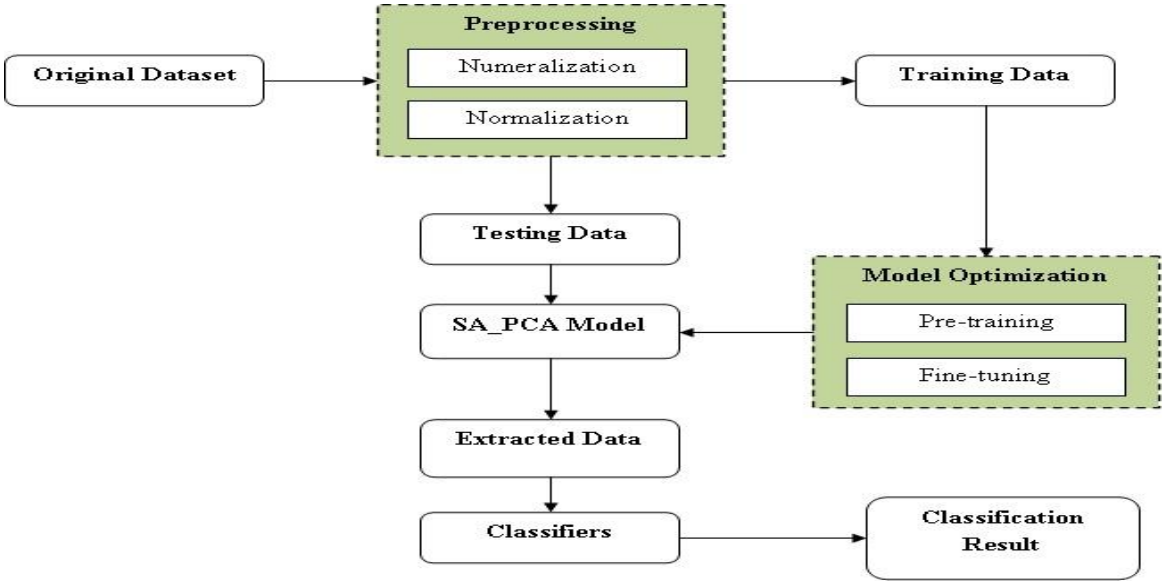

Fig. 4 Proposed SA_PCA Model

B. Dataset

Several public datasets are used in IDS that are based on KDD99. The advancement of the existing dataset named NSL-KDD is used in our experimental purposes. The dataset contains a total of 22543 test-samples and 125973 training-samples which include four types of attack samples and these are Probing attacks (Probe), User to root attacks (U2R), Denial of service attacks (DoS), and Remote to Local attacks (R2L) which is shown in Table 1. The training dataset is used to train the proposed model, and the test dataset is to test the performance of the detection possibility of the trained model [26].

Table 1 Specifications of NSL-KDD Dataset

Data Type		Sample Size	
		Testing-Set	**Training-Set**
Standard		67743	9591
Attack	U2R	152	120
	R2L	1295	2854
	Probe	11856	2400
	DoS	44927	7578
Total		125973	22543

C. Preprocessing

This is the first process of the proposed model for the NSL-KDD dataset that holds about 41 features that are classified into 0-1 type features, symbolic features, and percentage type features. Here, the feature Num_outbound_cmds value for all is given 0 that is not useful for the classification process which is removed in this phase. Since, the proposed SA_PCA model input is numeric matrix we convert symbolic-features into numerical-features.

- **Numeralization Process**

The numeralization process is performed by using one-hot encoding. The NSL-KDD dataset has symbolic-features which includes 'Service', 'Protocol Type', and 'Flag'. Three separate symbolic-feature values are included in 'Protocol Type', 70 separate symbolic-feature values are included in 'Service', and 11 different symbolic-features are given in 'Flag'. Therefore, once numeric processing is completed 121-dimensional features are extended in NSL-KDD dataset.

- **Normalization Process**

The result comparison is facilitated by the maximum and minimum normalization technique that denoted by the equation 9 which feature values are normalized in NSL-KDD dataset. The F_{max} denoted as maximum value of the original dataset and F_{min} is defined as minimum, the original feature is denoted by F and F_{norm} is defined as normalized-feature value.

$$F_{norm} = \frac{F - F_{min}}{F_{max} - F_{min}} \tag{9}$$

In this phase, the remaining features of NSL-KDD dataset is taken after the preprocessing step is completed. The 41-dimension features are extended to 121 dimensions and number of input-layer neurons is selected for SA_PCA. The parameters used for the simulation is given in Table 2. The features of the dataset SA_PCA model are given in Table 3.

Table 2 Simulation Parameters of SA_PCA

Model	Framework	Values
SA_PCA	Number of Nodes in Input-Layer	121
	Neurons in 1st Hidden-Layer	80
	Neurons in 2nd Hidden-Layer	75
	Neurons in 3rd Hidden-Layer	45
	Neurons in 4th Hidden-Layer	25
	Neurons in Output-Layer	5
	Sparse Parameter	0.05
	Size of the Batch	200
	PCA	-

Table 3 Features of the Dataset

S.No.	Feature Name
1	Protocol_Type
2	Time Duration
3	Flag
4	Service
5	DST_Bytes
6	SRC_Bytes
7	HOT
8	COUNT
9	Num_Root
10	Num_Compromised

11	SRV_diff_Host_rate
12	SRV_Count
13	Error_Rate

Table 3 shows the extracted feature-set after the proposed SA_PCA model is applied in which the most important features are selected. Totally 13 features are extracted out of 41 feature-set each which accessed using the neural network model of sparse auto-encoder and the principal components of each variable. The type of the features are also given in which it is a continuous or discrete is analyzed which could help to improve the performance of the classifiers.

D. Metrics

The experimental results are measured using the metrics of confusion matrix. Table 4 shows the significant of the confusion matrix. From Table 4, True Positive (TP) specifies number of correctly classified normal instances, True Negative (TN) indicates number of attack instances that correctly classified, False Positive (FP) identifies number of normal attacks incorrectly, and False Negative (FN) indicates incorrect number of attack records [27].

Table 4 Representation of Confusion Matrix

Typical Class		**Predicted Class**	
		Normal	Attack
Original Class	Normal	True Positive	False Positive
	Attack	False Negative	True Negative

Three main metrics are used for simulation results and these are Detection Rate (DR), False Positive Rate (FPR), and Accuracy and the formulas used for these metrics,

Accuracy is give condition of the precision on many use cases. Be that as it may, a great deal of times the precision of the system we are building probably won't be attractive or probably won't take us to the best positions on the pioneer load up in information science rivalries.

$$Accuracy = \frac{TN+TP}{TP+TN+FP+FN} \quad \text{---------- (i)}$$

Detection ratio gives a proportion of the testing adequacy and determined as a proportion of deformities found preceding discharge and after discharge by clients.

$$Detection\ Ratio = \frac{TP}{FN+TP} \quad \text{---------- (ii)}$$

False Alert Rate is an incorrect radar target recognition choice brought about by clamor or other meddling signs surpassing the identification limit.

$$False\ Alarm\ Rate = \frac{FP}{FP+TN} \quad \text{---------- (iii)}$$

V. Results And Discussions

The performance is evaluated using the proposed SA_PCA method by analyzing different experiments on NSL-KDD and KDD 99 datasets. The machine learning (ML) classifiers are used for evaluating the effectiveness of the extracted features using proposed extraction method SA_PCA with existing named as classifiers are Support Vector Machine (SVM), K-Nearest Neighbor (KNN) and PCA. The proposed SA_PCA method sustains better results and extracts the important feature that could help in improving the performance.

a) Comparison Proposed Method with Different Datasets

The proposed SA_PCA method is used for the comparison with other algorithms. The overall classification and performance of the proposed SA_PCA method is compared with other existing methods which shown in Table 5 in terms of accuracy, False Positive Rate and Detection Rate using NSL-KDD dataset. Table 6 shows the classification performance by the proposed method using KDD 99 dataset. Table 7 shows the five-category classification comparison with proposed method. The tables show that the proposed method has a better experiment results in terms of detection rate and accuracy that other state-of-art techniques. As of now, the training samples are less when compare with other existing classifiers but the proposed method gives

accuracy of 98.6%, detection rate 98.45%, and fewer false alarms rate which is about 3.12% is compared with NSL-KDD Datasets.

Table 5 Comparison using NSL-KDD Dataset

Methods	Accuracy (%)	Detection-Rate (%)	False Alarm Rate (%)
SVM	95.7	95.32	3.24
KNN	95.68	94.78	4.37
PCA	92.14	91.92	6.54
Proposed SA_PCA	98.6	98.45	3.12

Table 6 Comparison using KDD 99 Dataset

Methods	Accuracy (%)	Detection-Rate (%)	False Alarm Rate (%)
SVM	93.75	93.45	5.43
KNN	91.29	91.12	5.28
PCA	96.85	95.86	3.72
Proposed SA_PCA	98.4	98.12	3.43

The multi-classification evaluation based on Normal, U2R, R2L, Probe, and DoS are shown in Table 7. The proposed algorithm shows better results when comparing with other classifiers used earlier [28]. The different category classification results shown that detects different attacks are Normal has an accuracy of 98.91%, DoS has 98.6%, R2L has 92.45%, U2R has 85.73%, and Probe has 93.42%.

Table 7 Comparison based on Attacks

Algorithms	Normal	Probe	U2R	R2L	DoS
KNN	98.38	97.27	60.34	78.47	96.72
SVM	96.45	87.32	74.76	53.42	97.82
PCA	97.12	83.36	69.72	78.43	98.14
Proposed SA_PCA	98.91	93.42	85.73	92.45	98.6

VI. Conclusion

In this paper, a hybrid feature extraction method named SA_PCA is proposed for extracting the certain features to improve the performance in terms of accuracy, detection rate, and false alarm rate. Several researchers have used many learning methods for large volume of data to obtain the classification performance based on five-category which includes, Normal, Probe, U2R, R2L, and DoS. From the simulation results, the proposed SA_PCA method shows a better classification performance when compared with other classifiers. The SA_PCA obtain 98.6% of accuracy, 98.45% of detection rate, and 3.12% of false alarm rate.

References

[1]. John McHugh, *Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory, ACM Transactions on Information and System Security, 3(4),* 2000, 262-294.

[2]. P. Ravi Kiran Varma, V. Valli Kumari, and S. Srinivas Kumar, *A Survey of Feature Selection Techniques in Intrusion Detection System: A Soft Computing Perspective, Progress in Computing, Analytics and Networking, Singapore,* 785-793, 2018.

[3]. Ngoc Tu Pham, Ernest Foo, Suriadi Suriadi, Helen Jeffrey and Hassan Fareed M Lahza, Improving performance of intrusion detection system using ensemble methods and feature selection, 2018.

[4]. Kadurin A, Aliper A, Kazennov A, Mamoshina P, Vanhaelen Q, Khrabrov K and Zhavoronkov *A, The cornucopia of meaningful leads: Applying deep adversarial autoencoders for new molecule development in oncology, 8(7),* 2017, 10883-10890.

[5]. Rui Zhao, Ruqiang Yan, Zhenghua Chen, Kezhi Mao, Peng Wang, and Robert X. Gao, *Deep learning and its applications to machine health monitoring: A survey, 14(8),* 2016.

[6]. Khaled Alrawashdeh, and Carla Purdy, Toward an online anomaly intrusion detection system based on deep learning, IEEE International Conf. on In Machine Learning and Applications, 195-200, 2016.

[7]. Jin Wook Kim, Nara Shin and Sang Hyun Kim," Method of intrusion detection using deep neural network", In Big Data and Smart Computing, IEEE International Conf., 2017, 313-316.

[8]. Sasanka Potluri, and Christian Diedrich, Accelerated deep neural networks for enhanced Intrusion Detection System, In Emerging Technologies and Factory Automation (ETFA), IEEE International Conference, Berlin, 2016, 1-8.

[9]. Ahmad Javaid, Quamar Niyaz, Weiqing Sun, and Mansoor Alam, A deep learning approach for network intrusion detection system, Proc. of the 9th EAI International Conf. on BIONETICS, New York, 2015, 21-26.

[10]. Caelos Garcia Cordero, Sascha Hauke, Max Mühlhäuser and Mathias Fischer, Analyzing flow-based anomaly intrusion detection using Replicator Neural Networks, In Privacy Security and Trust, 14th Annual Conf., Germany, 2016, 317-324.

[11]. Lina You, Yujun Li, Yue Wang, Jie Zhang, and Yang Yang, A deep learning-based RNNs model for automatic security audit of short messages, 16th International Symposium on Communications and Information Technologies (ISCIT), China, 2016, 225-229.

[12]. Yao Wang, Wan Dong Cai, and Peng Cheng Wei, *A deep learning approach for detecting malicious JavaScript code, Security and Communication Networks, 9(11),* 2016, 1520-1534.

[13]. N. Senthil Murugan and G. Usha Devi, "Feature extraction using LR-PCA hybridization on twitter data and classification accuracy using machine learning algorithms", Cluster Computing, pp. 1-10, 2018.

[14]. N. Senthil Murugan and G.Usha Devi, *Detecting Streaming of Twitter Spam Using Hybrid Method, Wireless Personal Communications, 103(2),* 2018, 1353-1374.
[15]. Daniels Brauckhoff, Kave Salamatian and Martin May, Applying PCA for traffic anomaly detection: Problems and solutions, Proc. of IEEE INFOCOM, 2009, 2866-2870.
[16]. Haakon Ringberg, Augustin Soule, Jennifer Rexford and Christophe Diot, *Sensitivity of PCA for traffic anomaly detection, ACM SIGMETRICS Performance Evaluation Review, 35(1),* 2007, 109-120.
[17]. Gang Wang, Jinxing Hao, Jian Ma and Lihua Huang, *A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering, Expert systems with applications, 37(9),* 2010, 6225-6232.
[18]. Seyed Mojtaba Hosseini Bamakan, Huadong Wang, Tian Yingjie and Yong Shi, *An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization, Neuro computing, 199,* 2016, 90-102.
[19]. Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda and Zhiyuan Tan, Building an intrusion detection system using a filter-based feature selection algorithm, IEEE transactions on computers, 65(10), 2016, 2986-2998.
[20]. Opeyemi Osanaiye, Kim Kwang Raymond Choo, Ali Dehghantanha, Zheng Xu, and Mqhele Dlodlo, *Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing, EURASIP Journal on Wireless Communications and Networking,* 2016.
[21]. Arman Tajbakhsh, Mohammad Rahmati and Abdolreza Mirzaei, *Intrusion detection using fuzzy association rules, Applied Soft Computing, 9(2),* 2009, 462-469.
[22]. Binghao Yan and Guodong Han, Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system, IEEE Access, Zhengzhou, China, 2018, 41238-41248.
[23]. Wathiq laftah Al-Yaseen, Zulaiha Ali Othman and Mohd Zakree Ahmad Nazri, *Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system, 67,* 2017, 296-303.
[24]. StauRalf C.demeyer, *Applying long short-term memory recurrent neural networks to intrusion detection, South African Computer Journal, 56(1),* 2015, 136-154.
[25]. Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda and Zhiyuan Tan, *Building an intrusion detection system using a filter-based feature selection algorithm, IEEE transactions on computers, 65(10),* 2016, 2986-2998.
[26]. Chun Guo, Yuan Ping, Nian Liu and Shou shan Luo, *A two-level hybrid approach for intrusion detection, 214,* 2016, 391-400.
[27]. Wei Wang, Yiqiang Sheng, Jinlin Wang and Xuewen Zeng, *HAST-IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,* 2018, 1792-1806.
[28]. Seyed Mojtaba Hosseini Bamakan, Huadong Wang, Tian Yingjie and Yong Shi, *An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization, 199,* 2016, 90-102.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

K. Nandha Kumar. " A Hybrid Feature Extraction Method For Network Intrusion Detection System" IOSR Journal of Computer Engineering (IOSR-JCE) 21.3 (2019): 47-55.