AN EFFICACIOUS INTRUSION DETECTION SYSTEM FOR NETWORKS EXPLOITING RECURRENT NEURAL NETWORKS

D.Sobya

Associate Professor, Department of ECE, Rajarajeswari College of Engineering, Bangalore ,India.
E-mail: sobyadevaraj@gmail.com

Abstract-Intrusion detection in networks is an increasingly growing concern of information security because of its significance in modern IT infrastructure. A Network Intrusion Detection System (NIDS) aids system administrators in detecting gaps in security of networks thus preventing malignant intrusions. Anyway, several issues occur when generating an adaptable and systematic NIDS for the attacks which cannot be predicted. In this paper, a Recurrent Neural Network (RNN) depending on Intrusion Detection System (IDS) is introduced and analysed. The deep learning based RNN is utilized for classification as well as detects the count of neurons and various impacts of the rate of learning on accuracy. The NSLKDD dataset is utilized for the training of the proposed system and is tested for evaluating the performance in detecting intrusions. The comparisons of the obtained accuracy of the RNN are performed with existing classifiers and the experimental results showed promising outputs for real world application in intrusion detection systems.

Keywords: IDS, Recurrent neural network,Long Short Term Memory, GRU, FPR

1 INTRODUCTION

The internet has evolved as an efficient portion in our day-to-day life. Meanwhile various forms of cyber-attacks are quite common in the information handled by the internet [1]. At present, in network environment of the internet, different attacks in networks are regularly updated which increases the level of impacts as well as the network security issues [2]. Hence, the need for generating an effective protection approach against different network attacks to ensure safety and information security has been regarded as a major concern. To tackle this, Intrusion Detection Systems (IDS) are utilized which recognize malignant attacks with the analysis of traffic in networks and contribute to the security of networks [3].

Intrusion detection in networks denotes the process of observing and distinguishing intruded network activities which adversely affects the security of networks from the generally expected network behaviour [4, 5]. Depending on the behaviour of intrusions, the detection is divided as network-based intrusion detection system (NIDS) as well as host-based intrusion detection system (HIDS). An IDS system that utilizes network behaviour is termed as NIDS. The behaviours of network are gathered by its component through mirroring with networking devices, like routers, switches as well as network taps and analysed for identifying attacks as well as feasible attacks occurred in network traffic. An IDS system that utilizes the functionalities of system as different log files operating on the host computer present locally for detecting attacks is called as HIDS [6].

NIDS is a strong security tool that can defend against complicated attacks as well as threats. Yet, they face several issues and challenges due to the following reasons: (1) Variability and diversity of malignant attacks and threats. (2) Traditional machine learning approaches generate certain issues like overfitting and increased bias because of irrelevant or redundant features as well as unbalanced class distribution of traffic in network. (3) Complexity in labelling the traffic dataset [7]. At present, artificial intelligence techniques are applied in NIDS and these detection approaches relying on artificial intelligence faces increasing demand and they generally utilize neural networks [8]. Various intrusion detection approaches based on artificial intelligence like techniques depending on statistical analysis, cluster analysis and deep learning exist. Of these techniques, intrusion detection depending on deep learning is widely used due to its rigid capabilities like self-learning, self-adaptation, improved generalization and the detection of malignant attacks [9]. Deep learning is an advanced form of machine learning that simplifies the functioning of different complicated concepts as well as relationships utilizing several levels of implementations. It has obtained huge success in various fields and hence it is widely utilized in intrusion detection [10, 11]. The deep learning techniques perform efficiently during the availability of huge number of samples and have the ability to boost its performance as the number of samples increases [12].

Feed forward Neural Network (FNN) is a simple type of deep learning based Artificial Neural Network (ANN) adopted for classifying intrusions thus identifying abnormal data packets. But, their accuracy value varies with respect to the nature of attacks and generated inefficient results in detecting temporally correlated attacks [13, 14]. Subsequently, FC-ANN was proposed which introduced fuzzy clustering concepts in artificial neural networks. Utilizing these concepts, the complete training set was partitioned into small, minimal-complicated subsets. Depending on such subsets, each neural network exhibited improved stability with increased detection accuracy. But, this approach is suitable for minimal frequency attacks [15]. Deep Belief Networks (DBN) are another category of deep learning models which are utilized for improving the accuracy during classification and prediction. Its performance can be optimized by identifying the appropriate depth as well as count of neurons per layer in DBN. In contrast, if the network of DBN is very much complex, the consumed training duration will be high and if the network is very much simple, and its accuracy will be affected [16, 17].

Deep Neural Network (DNN) is also utilized for the detection of intrusions in networks. In a complex network, DNN varies network parameters by back propagation as well as fine tuning approaches for handling the detection of network attacks in an efficient manner [18]. Even though, DNN possessed better overall detection ability, its detection ability is minimum when considering normal types. This requires the optimization of algorithms in DNN based approaches [19]. Considering all these factors, Recurrent Neural Networks (RNN) are utilized in this approach for the detection of intrusions in network.

An enhanced intrusion detection system is proposed in this paper using RNN as well as the classification performance is studied. The contributions of this methodology are given as,

- The detection of intrusion in networks and its classification is performed with improved accuracy.
- The total count of neurons and the impacts of various rate of learning on accuracy are determined.
- The resulting accuracy of the RNN is analysed with existing approaches, thus proving the efficiency of the proposed methodology.

The remaining paper is structured as: The related papers are illustrated in section 2, the proposed system is explained in section 3, the results are discussed in section 4, and conclusion is narrated in section 5.

2 RELATED WORKS

Farrukh et al [20] introduced a deep learning concept of two stage for enhanced detection of intrusion in network depending on an auto-encoder which is stacked adopting soft-max classifier. It comprised two stages of decision: One stage that identifies the traffic in network as regular or irregular using a probability score value. This is then utilized as an extra function in the finally concluded decision stage to detect the attack types. This methodology learned automatically and efficiently as well as performed beneficial representation of features from vast quantities of unlabelled data along with its identification.

Pan et al [21] presented an approach which is systematized as well as automatized for building a hybrid IDS for learning temporal specifications which are state-based regarding scenarios of power systems that include various distractions, regulating operations as well as cyber-attacks. Common path mining which is a methodology of data mining concept was utilized for the automatic and accurate learning of patterns. The proposed approach performed accurate classification and effective implementation as well as validation of the prototype was performed.

Sana et al [22] developed a lightweight strategy for the detection of attacks exploiting a supervised machine learning-dependent support vector machine (SVM) for detecting an adversary that attempts for injecting irrelevant data into the IoT network. The simulated outputs revealed that the proposed SVM-based classifier, designed by combining two or three incomplex parameters, has the ability in performing satisfactory manner related to the accuracy of classification as well as time for detection.

Chuanlong et al [23] explored the way for modelling a system for detection of intrusion depending deep learning, and an approach for the detection of intrusion utilizing recurrent neural networks (RNN-IDS) is proposed. Furthermore, the model's functioning was analysed in binary and multiclass classification, as well as how the count of neurons as well as rate of learning influence the model's functioning. On benchmark data set, this approach is compared with other existing approaches.

Jin et al [24] proposed deep convolutional generative adversarial networks (DCGAN) that permitted the extraction of features, further generated updated training-sets with the raw data learning. Since the samples which are attacked are typically time sequence data of intra-dependent, long short-term memory (LSTM) is utilized for learning the characteristics of intrusion behaviours in network automatically. The LSTM algorithm depends on the outcome of the prior operations and hence parallelizing the LSTM network learning and its training is difficult.

3 PROPOSED SYSTEM

Recurrent neural networks comprises of hidden layer, output layer and input layer in which the hidden layer performs the major task. The RNN system generally possess single way information flow from input to hidden, as well as the blend of information flow through single way from the prior temporary concealment layer to the present hiding layer as given in figure 1. The hidden layer is considered as the complete network's storage that maintains the end-to-end information. On unfolding RNN, it is found that RNN characterizes deep learning and is utilized for supervised classification learning.

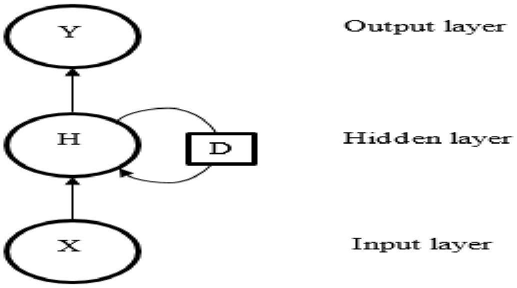


Figure 1 Recurrent Neural Networks

3.1 Modeling of RNN

RNN utilizes a directional loop which has the ability to store the previous information and this information can be applied to present output, which is considered to be the major variation from conventional FNNs. Prior outputs are also connected to present output of the series, and there exists connections among the nodes within hidden layers. The process flow of the utilized RNN for the detection of intrusion is indicated in figure 2.

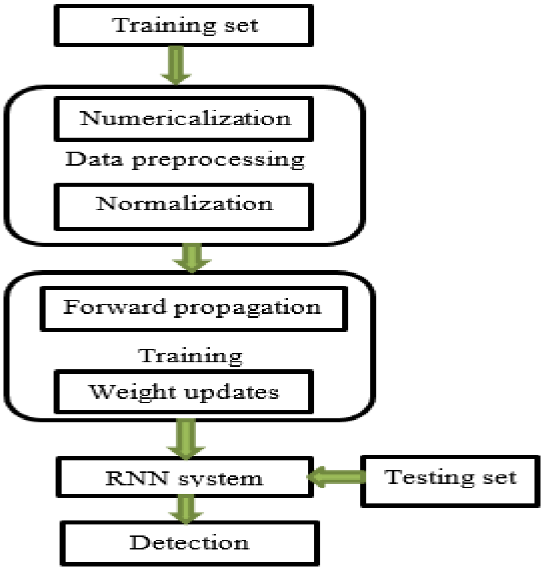


Figure 2 Process flow of proposed RNN.

3.2Preprocessing Of Data

3.2.1 Numericalization

In the utilized NSL-KDD dataset, 38 numeric features as well as 3 nonnumeric features are present. Since the RNN-IDS input has to be in a matrix form of numeric, the conversion of features which are nonnumeric, like 'protocol_type', 'service' as well as 'flag' features, is necessary. Let us consider the 'protocol_type' which has three kinds of parameters, 'tcp', 'udp', 'icmp', the corresponding numeric values of this feature are coded as (1,0,0), (0,1,0) and (0,0,1). Also, the 'service' has attributes of 70 kinds, 'flag' has attributes of 11 kinds. Thus, prior transformation and the mapping of dimensional features equalling to 41to dimensional features equalling to 122 occurs.

3.2.2 Normalization

Initially, consider the features like 'duration[0,58329]', 'src_bytes[0,1.3 × 109]' as well as 'dst_bytes[0,1.3 × 109]', in which the difference of the high as well as low values has increased option, the logarithmic scaling concept has to be applied for scaling to receive the ranges of 'duration[0,4.77]', 'src_bytes[0,9.11]' , 'dst_bytes[0,9.11]'. Next, the mapping of each feature value is done with [0,1] as given in (1), in which max indicates the greater value, min indicates lower value for every feature.

$$a_i = \frac{a_i - min}{max - min} \tag{1}$$

33 Training

There are two major events in the training of RNN namely, Forward Propagation as well as Back Propagation. Forward Propagation performs the estimation of output values, and Back Propagation passes the residuals which are gathered for updating the weights. Consider $a_i(i = 1,2, \dots .n)$, which denotes the samples for training, $h_i(i = 1,2, \dots .n)$, denoting a series of hidden layers , $\widehat{b_\imath}(i = 1,2, \dots n)$ indicating series of predictions, W_{ha}denotes weight matrix of input-to-hidden layer, W_{hh} defines weight matrix of hidden-to-hidden layer, W_{bh} denotes weight matrix of hidden-to-output layer, q_h, q_b indicate vector biases. Consider η as the rate of learning and p as the number of present iterations and the series of labels $b_i(i = 1,2, \dots .n)$.

```
**Algorithm for training**
**Input** $a_i(i = 1,2, \dots . n)$
**Output** $\widehat{b_\iota}$
   For $i$ from 1 to $n$ do
                  $ti = W_{haai} + W_{hhhi-1+qh}$
$hi$ = sigmoid $(ti)$
$si$ = $W_{bhhi+qb}$
$\widehat{b_\iota}$ = softmax $(si)$
   end for
**Algorithm for weight updates**
**Input** $\langle y_i, \widehat{y_\iota} \rangle (i = 1,2, \dots . n)$
**Initialization** $\theta = \{W_{ha}, W_{hh}, W_{bh}, q_h, q_b\}$
**Output**          $\theta = \{W_{ha}, W_{hh}, W_{bh}, q_h, q_b\}$
      for $i$ from $k$ downto 1 do
            Estimate cross entropy within output as well as label: $L(y_i, \widehat{y_\iota}) \leftarrow \sum_i \sum_j b_{ij} \, log(\hat{b}_{ij}) + (1 - b_{ij}) \log(1 - \widehat{b_{\iota J}})$
            Evaluate partial derivative considering$\theta_i$:$\delta_i \leftarrow \frac{dL}{d\theta_i}$
            Updated weight: $\theta_i \leftarrow \theta_{i\eta} + \delta_i$
        end for
```

3.4 RNN-Based LSTM And GRU

The LSTM system depending on RNN utilizes a remodelled cell for hidden layer for capturing increased-duration dependencies related to input series. It adopts the methodology of gating units for controlling the flow of information as well as study dependencies of long duration adaptively. The internal state's update comprises of the element from external input and the element from the prior state. The framework of LSTM cell is given by figure 3.

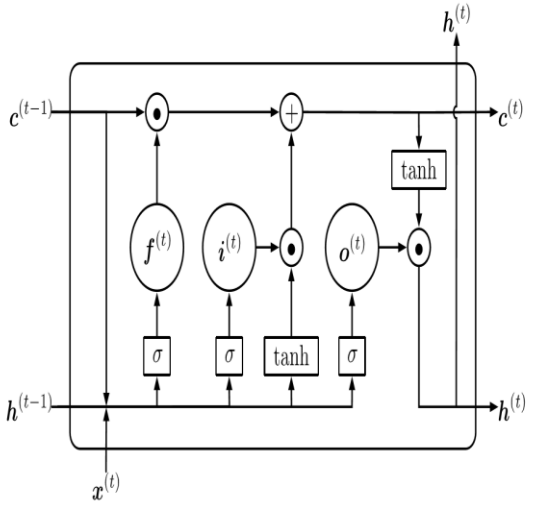


Figure 3 LSTM cell

The RNN based Gated Recurrent Unit (GRU) is framed with a two-gate model for imitating the performances of the three gates in LSTM. It also eradicates the specific internal state in the LSTM cell. The framework of GRU cell is given in figure 4.

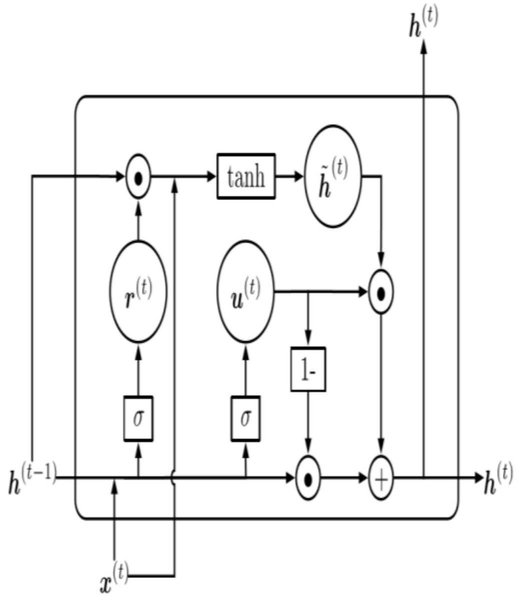


Figure 4GRU cell

Both LSTM and GRU model generated better performance adopting RNN related to the ease of training of the model and the accurate values for the results of classification.

4 RESULTS AND DISCUSSION

4.1 Dataset

The NSL-KDD dataset is commonly utilized for the methods for detection of intrusion. It tackles the intrinsic expendable issues of details of KDD Cup 1999 dataset and keeps the count of details valid in training set as well as testing set, and hence the classifier do not provide additional periodic details. The dataset includes the KDD Train+ dataset as training set , testing set includes KDD Test+ as well as KDDTest−21 datasets, which consists of various normal as well as attack details.

4.2 Evaluation Metrics

The working ability of the utilized RNN model is measured by the indicator accuracy along with detection rate as well as false positive rate. The True Positive (TP) is equal to the details that are correctly eliminated, thus indicates the count of attacked details which are found as attacks. The False Positive (FP) is equal to the details that are inaccurately eliminated, indicating the count of normal details which are found as attacks. The True Negative (TN) is equal to details accurately admitted, and it indicates the count of normal details which are found as normal. The False Negative (FN) is equal to details which are incorrectly admitted, and it indicates the count of attacked details found as normal is given by table 1.

Table 1 Confusion matrix

Predicted class Original class	Attack	Normal
Attack	TP	FN
Normal	FP	TN

4.2.1 Accuracy

It denotes the percentage of the count of details classified accurately to the overall count of details.

$$Accuracy = \frac{TN + TP}{TN + FN + TP + FP}$$

4.2.2 True Positive Rate (TPR)

It is considered equal to Detection Rate (DR), and denotes the percentage of the count of details estimated accurately to the overall count of details with attacks.

$$TPR = \frac{TP}{FN + TP}$$

4.2.3 False Positive Rate (FPR)

It denotes the percentage of the count of details eliminated inaccurately to the overall count of normal details.

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

The confusion matrix of the proposed RNN dependent intrusion based detection system on the KDD Test+ testing set is given in table 2. The total count of normal details and the details with attacks are indicated in the confusion matrix.

Table 2 Confusion matrix

Predicted class Original class	Attack	Normal
Attack	9362	3471
Normal	298	9413

The proposed RNN shows improved performance when compared to existing methods and the obtained accuracy values are illustrated in table 3.

Table 3 Comparison of accuracy

	Naïve Bayes [25]	Random tree [26]	Multilayer perception [27]	J48 [28]	NB tree [29]	SVM [30]	Random forest [31]	RNN
KDD Test+	76.5	81.5	77.4	81	82	69.5	80.6	83.2
KDD Test-21	55.7	58.5	57.3	63.9	66.1	42.2	63.2	68.5

The characteristic plot of the accuracy values of existing classifiers and the proposed RNN is given in figure 5. From the graph it is evident that the proposed approach generated efficient results.

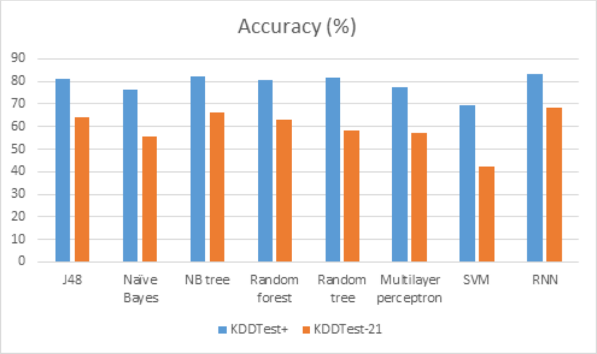
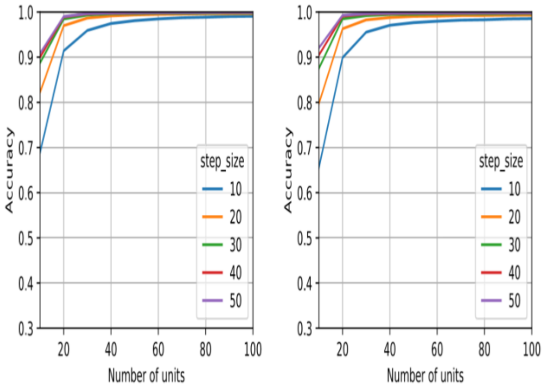


Figure 5 Comparison of accuracy

The obtained values indicate that the intrusion detection system of RNN generated improved results regarding classification as well as detection of intrusions. The accuracy rate obtained is high when compared to other existing detection approaches.



(a) (b)

Figure 6 Accuracy for RNN based (a) LSTM (b) GRU

From the figure 6 it is clear that improved accuracy is obtained with RNN based LSTM and GRU providing the recurrent layer with sufficiently huge number of hidden units even with increased step size.

5 CONCLUSION

The proposed RNN system is strongly capable for intrusion detection as well as classification with improved accuracy. When compared with conventional classification approaches, the performance attains an increased accuracy rate as well as rate of detection with minimal FPR. It effectively identifies the type of intrusion thus providing potent detection of intrusion. RNN based LSTM and GRU are also analysed generating improved accuracy. In future, studies can concentrate on reducing the training time.

References

[1] Kehe Wu;Zuge Chen;Wei Li, “A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks”, IEEE Access, Vol. 6, pp. 50850 – 50859, 2018.

[2] Ali, M. H., Al Mohammed, B. A. D., Ismail, A., & Zolkipli, M. F, “A new intrusion detection system based on fast learning network and particle swarm optimization”, IEEE Access, Vol. 6, pp. 20255-20261, 2018.

[3] Wei Wang;Yiqiang Sheng;Jinlin Wang;Xuewen Zeng;Xiaozhou Ye;Yongzhong Huang;Ming Zhu, “HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection”, IEEE Access, Vol. 6, pp. 1792 – 1806, 2018.

[4] Sheraz Naseer;Yasir Saleem;Shehzad Khalid;Muhammad Khawar Bashir;Jihun Han;Muhammad Munwar Iqbal;Kijun Han, “Enhanced Network Anomaly Detection Based on Deep Neural Networks”, IEEE Access, Vol. 6, pp. 48231 – 48246, 2018.

[5] Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z, “Building an intrusion detection system using a filter-based feature selection algorithm”, IEEE transactions on computers, Vol. 65, no. 10, pp. 2986-2998, 2016.

[6] Marteau, P. F, “Sequence covering for efficient host-based intrusion detection”, IEEE Transactions on Information Forensics and Security, Vol. 14, no. 4, pp. 994-1006, 2018.

[7] Hongyu Yang;Fengyan Wang, “Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network”, IEEE Access, Vol. 7, pp. 64366 – 64374, 2019.

[8] Ying Zhang;Peisong Li;Xinheng Wang, “Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network”, IEEE Access, Vol. 7, pp. 31711 – 31722, 2019.

[9] Sydney Mambwe Kasongo;Yanxia Sun, “A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System”, IEEE Access, Vol. 7, pp. 38597 – 38607, 2019.

[10] Wang, Z, “Deep learning-based intrusion detection with adversaries”, IEEE Access, Vol. 6, pp. 38367-38384, 2018.

[11] Safa Otoum;Burak Kantarci;Hussein T. Mouftah, “On the Feasibility of Deep Learning in Sensor Network Intrusion Detection”, IEEE Networking Letters, Vol. 1, no. 2, pp. 68 – 71, 2019.

[12] Shone, Nathan, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi, "A deep learning approach to network intrusion detection" , IEEE transactions on emerging topics in computational intelligence, Vol. 2, no. 1, pp. 41-50, 2018.

[13] Raja, S., & Ramaiah, S, “An efficient fuzzy-based hybrid system to cloud intrusion detection”, International Journal of Fuzzy Systems, Vol. 19, no. 1, pp. 62-77, 2017.

[14] Benmessahel, I., Xie, K., Chellal, M., & Semong, T, “A new evolutionary neural networks based on intrusion detection systems using locust swarm optimization”, Evolutionary Intelligence, Vol. 12, no. 2, pp. 131-146, 2019.

[15] Peng Wei;Yufeng Li;Zhen Zhang;Tao Hu;Ziyong Li;Diyang Liu, “An Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network”, IEEE Access, Vol. 7, pp. 87593 – 87605, 2019.

[16] Xu, C., Shen, J., Du, X., & Zhang, F, “An intrusion detection system using a deep neural network with

gated recurrent units", IEEE Access, Vol. 6, pp. 48697-48707, 2018.

[17] Yang, Y., Zheng, K., Wu, C., Niu, X., & Yang, Y, "Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks", Applied Sciences, Vol. 9, no.2, 2019.

[18] Xianwei Gao;Chun Shan;Changzhen Hu;Zequn Niu;Zhen Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection", IEEE Access, Vol. 7, pp. 82512 – 82521, 2019.

[19] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S, "Deep learning approach for intelligent intrusion detection system", IEEE Access, Vol. 7, pp. 41525-41550, 2019.

[20] Farrukh Aslam Khan;Abdu Gumaei;Abdelouahid Derhab;Amir Hussain, "A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection", IEEE Access, Vol. 7, pp. 30373 – 30385, 2019.

[21] Pan, Shengyi, Thomas Morris, and Uttam Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems" IEEE Transactions on Smart Grid, Vol. 6, no. 6, pp. 63104-3113, 2015.

[22] Jan, Sana Ullah, Saeed Ahmed, Vladimir Shakhov, and Insoo Koo, "Toward a lightweight intrusion detection system for the internet of things", IEEE Access, Vol. 7, pp. 42450-42471, 2019.

[23] Chuanlong Yin;Yuefei Zhu;Jinlong Fei;Xinzheng He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks", IEEE Access, Vol. 5, pp. 21954 – 21961, 2017.

[24] Jin Yang;Tao Li;Gang Liang;Wenbo He;Yue Zhao, "A Simple Recurrent Unit Model Based Intrusion Detection System With DCGAN", IEEE Access, Vol. 7, pp. 83286 – 83296, 2019.

[25] Jabbar, M. A., & Aluvalu, R, "RFAODE: A novel ensemble intrusion detection system", Procedia computer science, Vol.115, pp. 226-234, 2017.

[26] Aljawarneh, S., Aldwairi, M., & Yassein, M. B, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model", Journal of Computational Science, Vol. 25, pp. 152-160, 2018.

[27] Hajimirzaei, Bahram, and Nima Jafari Navimipour, "Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm", ICT Express, Vol. 5, no. 1, pp. 56-59, 2019.

[28] Panigrahi, R., & Borah, S, "Rank allocation to J48 group of decision tree classifiers using binary and multiclass intrusion detection datasets", Procedia computer science, Vol. 132, pp. 323-332, 2018.

[29] Kevric, J., Jukic, S., & Subasi, A, "An effective combining classifier approach using tree algorithms for network intrusion detection", Neural Computing and Applications, Vol. 28, no. 1, pp. 1051-1058, 2017.

[30] Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection", IEEE Access, Vol. 6, pp. 52843-52856, 2018.