TECH-KNOWLEDGE JOURNAL

Improving Intrusion Detection System Based On Long Short-Term Memory and Principal Component Analysis

Bilal Mohammed*, Ekhlas K. Gbashi
Department of Computer Science, University of Technology, Baghdad, Iraq
* cs.19.65@grad.uotechnology.edu.iq

Keywords: **Intrusion Detection Systems (IDS), Classification, Long Short-Term Memory (LSTM), Principal Component Analysis (PCA).**

ABSTRACT

Intrusion detection system is responsible for monitoring the systems and detect attacks, whether on (host or on a network) and identifying attacks that could come to the system and cause damage to them, that's mean an IDS prevents unauthorized access to systems by giving an alert to the administrator before causing any serious harm. As a reasonable supplement of the firewall, intrusion detection technology can assist systems to deal with offensive, the Intrusions Detection Systems (IDSs) suffers from high false positive which leads to highly bad accuracy rate. So, this work is suggested to implement (IDS) by using a Principal component analysis to select features and Long short-term memory for classification, the suggested model gives good results with accuracy rate reaching 81% was used in the classifications for the five classes (Normal, Dos, Probe, R2L, U2R). The system was implemented by using (NSL-KDD) dataset, which was very efficient for offline analyses systems for IDS.

1.0. INTRODUCTION

Intrusion detection systems is a security technique which analyses network systems and computer in real time to detect intrusions and manage responsive actions [1]. Signature and Anomaly are two major models that utilized in intrusion detection systems.

The anomaly is depending on the statistical description of programs or users which is mean detecting any activity deviating from the profile of normal behavior The Signature-based IDSs depends on gathering and saving the signature of known attacks in database [2] and it is different from classic security [3].

The very huge increase in networks and with the increase of devices and users, the computers suffer from attacks and security vulnerabilities which be difficult and expensive to be solved, so the best solution is intrusion detection system to control and monitor the traffic in network.

The paper revision for anomaly detection fully based on deep machine learning ways on different training and testing dataset. The suggested system was implemented by NSL-KDD dataset because of the problems in KDD99 dataset [4]. The Network Intrusion Detection System (NIDS) is estimate to know attacks which need a comprehensive data set that contains known and unknown behaviors [5].

This work proposes a network intrusion detection system which depends on Long Short-Term Memory to classify the normal and the attacks. The paper is arranged as follows: section two illustrates some

related works, section three shows Descriptions for the dataset as inclusive and substantive, section four explains the evaluation metrics, section five talk about PCA and six illustrates Long Short-Term Memory, section seven explain the steps of suggested system, section eight illustrates the experimental results and discussions and finally conclusions and future work.

2.0. RELATED WORK

Many recent systems depend on normal machine learning techniques. One public approach is to utilize ANN to build intrusion detection systems. Such as, the feed forward neural network is applied to build a classifier, and the back-propagation algorithm is utilized to train the network classifier [6].

Many of the common methods are used to detect intrusion in intrusion detection systems, such as Support vector machines [7], K-nearest neighbor (KNN), and Random forest (RF) [8]. [9] presented a hybrid IDS approach that utilizes the decision tree and the Support Vector Machine to combine anomaly attack detection and misuse attack detection on the NSL-KDD dataset, they evaluated their hybrid IDS. Use anomaly detection with the Naive Bayes (NB) and examined on the KDD99 [10]. Examined DARPA dataset by utilized Support Vector. Examine of KDD dataset by added the C4 and Self-Organization Map [11].

While great accuracy was achieved to some degree in the detection of security threats, some perfection is required, such as improving the accuracy and reducing the size of false alarms [12]. Popularize the capability of a multilayer perceptron (MLP) network similar to the layers in an attack that is evaluated on the KDD 99 dataset. For feature choice and classification, which are tested on the KDD dataset [13], LSTM-based deep learning approaches are proposed in the label.

Machine learning learn the particulars of TCP/IP attributes, but Deep learning is a part of machine learning that be complex because it consists of many layers and transit the TCP/IP in many layers. design this model that combine discretization and HNB classifier this approach focused on problems in intrusion detection and this model based on hidden layer in NB model for many class than can get better accuracy and high detection rate of attacks [14].

Newly, deep learning methods as a research hotspot have also been powerfully used in the development of intrusion detection systems. For intrusion detection, a proposed neural network classifier depends on Self-Taught Learning (STL) is proposed in [15]. According to [16], multi-channel LSTM assembles several features using different source features, like numeric-based, nominal-based, and binary-based.

In [17], the authors detected how to establish an (Intrusion Detection System) based on Recurrent Neural Network algorithm.

3.0. DATASET DESCRIPTION

Since 1999, the Knowledge Discovery and Data Mining (KDD'99), wildly used data set for the estimated of anomaly detection techniques [18]. Some investigators examine KDD99 but results were poor execution on the anomaly detection approach so the best solution was using new dataset which is NSL-KDD [18]. This dataset consists of chosen records of the all KDD data set. The Training dataset consists of (125,973) and test dataset consists of (22,544) samples each of sample contains 41 attributes either attacks or normal. Attacks in this dataset are split into: Root to Local (R2L), User to Root(U2R), Denial of service(DOS), Probe Attacks. The following shows some explanations for these attacks types:

I. *Dos:* It is a class of attack where the attacker restricts processing time of the resources so as to avoid the real user from obtaining those resources.
II. *R2L:* Attackers are not allowing access from a remote system.R2L attack is both categorized under network based and host-based (NIDS).
III. *U2R:* the attacker tries to gain the password of the user and then get into the system as a legitimate user and retrieve the data.
IV. *Probe:* The Attacker will exam the network to collect information and would make some penetrations in the next time.

In addition to these types we also have a class describing the Normal class. Table (1) shows the four types of attack in *NSL_ KDD* [19].

Table 1: Attacks in NSLKDD dataset

Intrusions	Intrusions Type
DOS	Back,Smurf,Teardrop,Pod,ProcesstableLand,Apache,Mailbomb,Udpstorm ,Neptune, Worm.
probe	Mscan,IPsweep,Satan,Saint ,Portsweep, Nmap.
R2L	Sendmail,Xsnoop,Ftp_write,hop,Imap,MultiNamed,Snmpgetattack,Guess _password,Phf,Snmpgue,Xlock,Httptunnel,Warezmaster,ss.
U2R	Xterm,Rootkit,Loadmodule,Ps,Buffer_overflow,Perl,Sqlattack

4.0. EVALUATION METRIC

It was nominated for applying a similar validation process of each one of the classifier percentages. A data-set with about the same class distributions and sizes has been considered. The classifier has been trained for each one of the folds with the use of the percentage for class. In this part, a clarification has been provided, which was based upon the measurement of the performance for the task of the machine learning classification, whereas the output may be comprising 2, or more classes. The 5 classes (i.e. the Dos, normal, probe, u2l, r2l) in current investigation, and the 6 distinct combinations of actual and predicted values [20,21], have been listed in Table (2).

Table 2: The different metric such as Accuracy, Precision, Recall

Metric	Eq.
Accuracy	$\frac{\text{TP+TN}}{\text{Total Number of Samples}} \times 100$ (1)
Precision	$\frac{\text{TP}}{\text{TP+FP}}$ (2)
Recall	$\frac{\text{TP}}{\text{TP+FN}}$ (3)
F-score	$2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}}$ (4)
False Positive Rate	$\frac{\text{FP}}{\text{FP+TN}}$ (5)
Area Under the ROC Curve (AUC)	$\int_0^1 \frac{\text{TP}}{\text{TP+FN}} \, \text{d} \, \frac{\text{FP}}{\text{TN+FP}}$ (6)

5.0. PRINCIPAL COMPONENT ANALYSIS

It is largely a statistical method for data analysis and pre-processing that has been widely applied in various fields of research [22, 23]. PCA is built to alter information in a diminished form and to retain the vast majority of the first variations to the beginning of the information present. In this paper, PCA is used on the basis of the highest correlation weight value to select features that affect data.

6.0. LONG SHORT-TERM MEMORY

It is a type of recurrent neural network capable of learning order dependence in sequence prediction problems? Recently LSTM used in speech recognition [24, 25], language modeling, translation, image captioning. The LSTM contains special units called memory blocks in the recurrent hidden layer. Each memory block in the original architecture contained an input and an output.

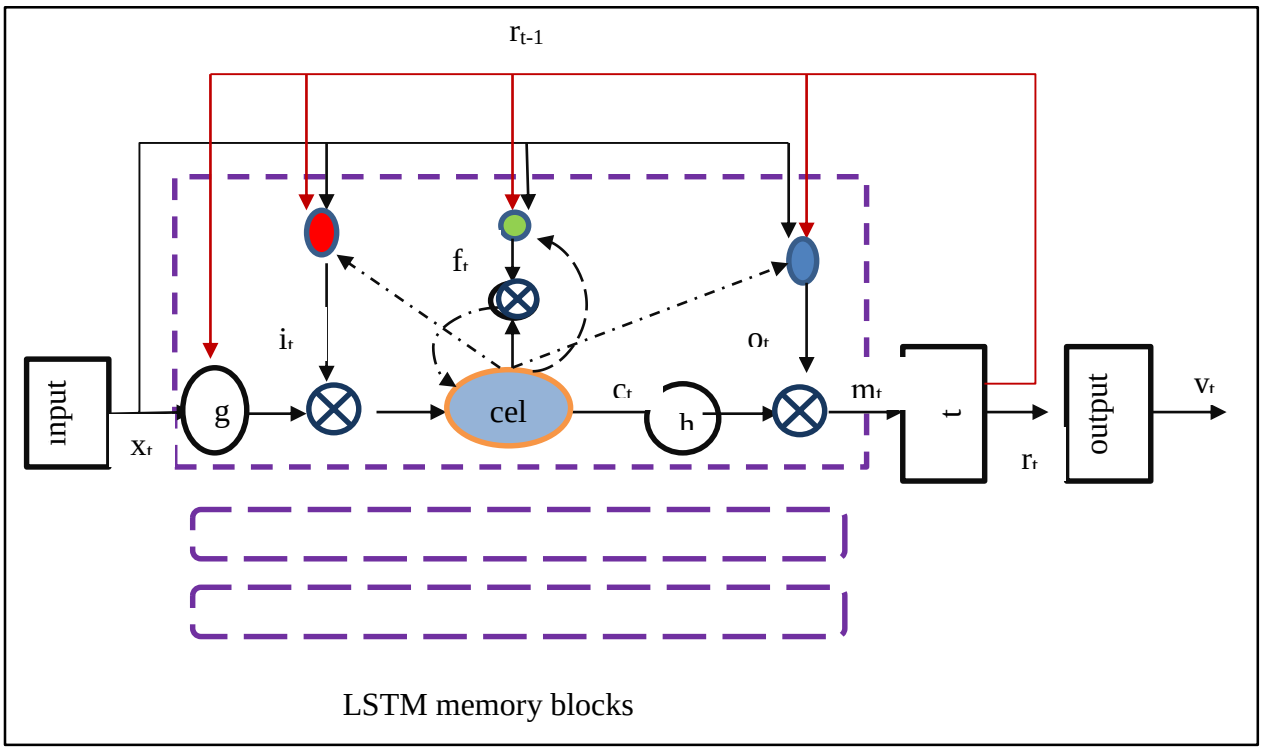

Fig. 1: LSTM architecture.

An LSTM network computes a mapping from an input sequence x = (x1, ..., xT) to an output sequence y = (y1, ..., yT) by calculating the network unit activations using the following equations iteratively from t = 1 to T [26]:

$$i_t = \sigma(W_{ix}x_t + W_{im}m_{t-1} + W_{ic}c_{t-1} + b_i) \quad (7)$$

$$f_t = \sigma\left(W_{fx}x_t + W_{fm}m_{t-1} + W_{fc}c_{t-1} + b_f\right) \quad (8)$$

$$c_t = f_t \odot c_{t-1} + i_t \odot g(W_{cx}x_t + W_{cm}m_{t-1} + W_{ic}m_{t-1} + b_c) \quad (9)$$

$$o_t = \sigma(W_{ox}x_t + W_{om}m_t + W_{oc}c_t + b_o) \quad (10)$$

$$m_t = o_t \odot h(c_t) \quad (11)$$

$$y_t = \emptyset(W_{y_m} m_t + b_y) \quad (12)$$

where the W terms denote weight matrices, the b terms denote bias vectors (bi is the input gate bias vector), σ is sigmoid function, and i, f, o, and c the input gate, forget gate, output gate are respectively and cell , all of which are the same size as the cell output activation vector m, is the element-wise product of the vectors, g and h are the cell input and cell output activation functions, generally and in this paper tanh, and φ is the network output activation function, SoftMax in this paper.

7.0. PROPOSED MODEL

The model of intelligent Network IDS was proposed with the structure of the hierarchical progressive network where in this model design; approach based on NSLKDD dataset was used. After preprocessing for dataset because this data is raw. Normalization was applied to make all features having values ranging from 0 to 1. The train set has been utilized to train model and the testing set has been utilized for the evaluation of the trained model. By applying the pca technique was used to select important features from Train set and these important features have used it with the test set at predict. After selecting features of train set, it was built a model for classification by using LSTM algorithm on the train set. Finally, evaluating the model by predicting with test set and compared results.

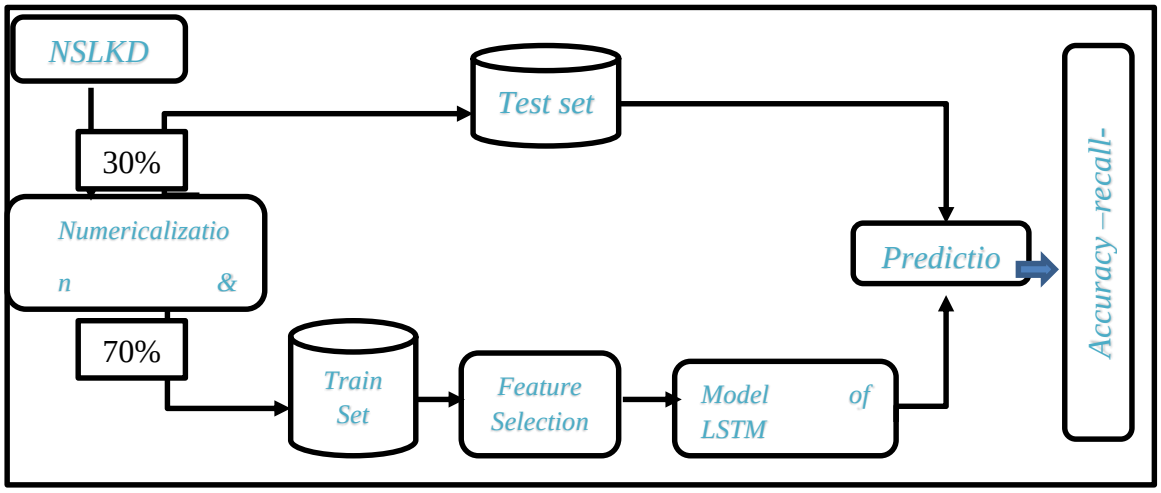

Fig. 2: Proposed model

7.1. Numericalization

For training and testing, the LSTM-based classification uses just numerical values. Therefore, to transform non-numerical values into numerical values, a pre-processing stage is required. In our pre-processing, two major tasks are:

1. The non-numerical attributes in the dataset Converting to numerical values. The features 2, 3 and 4 are the protocol type, service and flag were non-numerical. were converted to numerical data by make specific values to each variable (e.g. TCP = 1, UDP = 2 and ICMP = 3).
2. The attack types at the end of the dataset Convert into its numeric categories. Category 1 is to the normal attack, and 2, 3, 4 and 5 are make it to DoS, Probe, R2L and U2R attack kinds, respectively

7.2. Normalization

The features in the NSL-KDD datasets have either continuous or discrete values. The ranges of the values were different and this made them incomparable. The features were normalized by subtracting mean from all feature and dividing by its standard deviation, then normalized the test features using the mean and standard deviation of each feature from train datasets. Min-Max normalization way which is a linear transformation is utilized to scale data between (0,1). The following method is utilized to find the new value [27]:

$$X_n = \frac{X - X_{min}}{X_{max} - X_{min}} \qquad (13)$$

7.3. Training set & Test set

1. The training set: In this set, our LSTM architecture is trained using the known attacks.
2. The testing set: In this set, we have verified how the same architecture is working in case of unknown attacks

7.4. Features Selection

Feature selection is one of the essential and a lot utilized ways in data preprocessing for the intrusion detection system. It decreases the number of attributes, split redundant, irrelevant, or noisy data, and fetch the essential effects for the intrusion detection system**.** In this method, data is passed first, according to the PCA algorithm from NSLKDD. When using PCA as a feature selection method, the fundamental concept is to choose variables according to the degree of their coefficients (from highest to lowest). Note that PCA tries to substitute V (more or less relevant variables with R < V uncorrelated linear combinations of the original variables. Via their explained variance, these R principal components are rated by significance, and each variable corresponds to each component to a varying degree. Utilizing the largest variance criteria will be akin to features extracted, where the principal component is utilized rather than the original variables as new features. However, you can choose to keep just the first component and choose the S<V variables with the highest absolute coefficient; the number S can be dependent on the proportion of the number of variables (for example, holding only the highest 20% of the V variables).

7.5. Model of LSTM

The suggested model was a fully-connected network structure with 3 layers (Input, Hidden and Output). The input layer can specify the number of neurons or nodes in the layer as the first argument, In LSTM, there is an important feature which is return sequences, by default set to False, so there is a need to return sequences=True for adding more layers. Also, dropout as regularization technique is used to avoid over-fitting when training. Finally, in the output layer, the SoftMax function which takes output values between 0 and 1 as shown in Table 4 and Table 5.

Table 4: Adding each layer in LSTM

The input layer of data with 19 variables since important features that select from pca technique (the input_dim=19 argument)
The first hidden layer includes 64 nodes
The second hidden layer includes 64 nodes
The third hidden layer includes 64 nodes

The fourth hidden layer includes 64 nodes
The output layer has Dense= 5 nodes for multi-class classification and uses the softmax activation function.

Table 5: Algorithm (1) Model of LSTM

Input: Output: Classify the type of attack
Begins Step1: for t from 1 to m do Step2: tι=$\mathbf{c_t} \odot \mathbf{g}(\mathbf{W_{cx}x_t} + \mathbf{W_{cm}m_{t-1}} + \mathbf{W_{ic}m_{t-1}} + \mathbf{b_c})$ **Eq 9** Step3: st =$\boldsymbol{\sigma}(\mathbf{W_{ox}x_t} + \mathbf{W_{om}m_t} + \mathbf{W_{oc}c_t} + \mathbf{b_o})$ **Eq 10** Step**4**: $\mathbf{y_t}$=SoftMax(st) Step5: end for End

7.6. Prediction

In this final stage of the proposed system, the evaluation process works by applying the model that trains the training set on new groups and different from the training set, which is the test set by measuring the outputs, for example (Accuracy, Precision, Recall, F-score, False Positive Rate, to know the ability of the model to discover new states of the attacks.

8.0. EXPERIMENTAL RESULTS

In early 2015, Keras had the first reusable open-source Python implementations for developing and evaluating deep learning models.The system was implemented by (NSL -KDD) dataset. This work was implemented by the Python language. The NSL -KDD composed of 125,973 train set and 22,544 test set confined with 5 attacks.

In general, obtainable Network Intrusion Detection System by NSL -KDD dataset to make an Offline system and was to evaluate of work by recurrent neural network. The NSL -KDD was isolated automatically into train and test sets. For train set, most of the LSTM network topology showed train accuracy reached to 99%.

Table 6: Results of train set

Attack Type	Precision	Recall	F1-Score	Accuracy
DOS	99%	99%	94%	99%
Normal	99%	98%	97%	99%
probe	87%	75%	89%	99%
U2R	85%	95%	91%	97%
R2L	87%	98%	89%	79%

Table 6 shows the training set and the experiments display that after examining the outcomes of the data. It was found that the accuracy of each class in train set was very good. Dos was 99%, normal was 99%, probe was 99%, u2r was 97% and R2l was 97%. Detection rate was 99%, false alarm rate was 0.003% and False Negative Rate 0.004 % for Dos. Detection rate was 98%, false alarm rate was 0.013% and False Negative Rate 0.014% for normal. Detection rate was 99%, false alarm rate was 0.054% and False Negative Rate 0.003% for probe. Detection rate was 99%, false alarm rate was 0.00% and False Negative Rate 0.00% for U2r.Detection rate was 99%, false alarm rate was 0.00% and False Negative Rate 0.00% for r2l.

Table 7: Results of test set

Attack Type	Precision	Recall	F1-Score	Accuracy
DOS	76%	78%	77%	63%
Normal	79%	72%	71%	84%
probe	72%	77%	74%	70%
U2R	71%	87%	81%	70%
R2L	99%	99%	99%	72%

For test set shown in Table 7, the results of accuracy on test set were for Dos was 63%, normal was 84%, probe was 70%, u2r was 70% and R2l was 72%. Detection rate was 88%, false alarm rate was 0.521% and False Negative Rate 0.114% for Dos. Detection rate was 553%, false alarm rate was 0.060% and False Negative Rate 0.447% for normal. Detection rate was 90%, false alarm rate was 0.903% and False Negative Rate 0.094% for probe. Detection rate was 99%, false alarm rate was 0.00% and False Negative Rate 0.00% for U2r.Detection rate was 99%, false alarm rate was 0.00% and False Negative Rate 0.00% for r2l.

The operating characteristics of the receiver can be used to provide explanations for the required work to extract the results by providing the graphics shown in Figure 3. Blue color indicated to the evaluation process of training and Green color indicated the evaluation process of testing. The ROC curve of NSLKDD is shown in Figure 3. In most of the cases, LSTM was performed well with AUC utilized as standard metric. Which is indicating the fact that the LSTM has obtained the maximal true positive rate and lowest false positive rate in some cases approximate to 0.

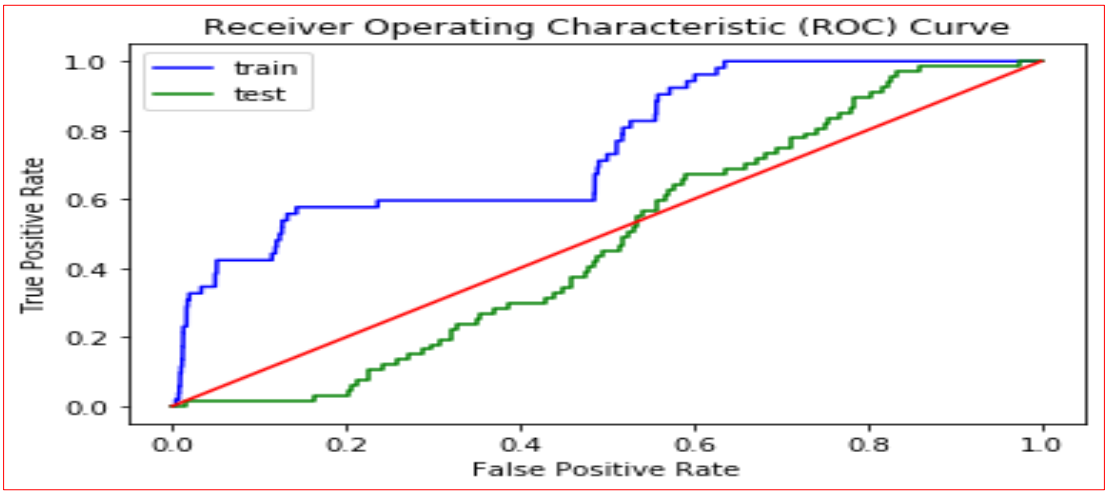

Fig. 3: Comparison performance IDS NSLKDD on AUROC curve by LSTM.

9.0. CONCLUSIONS AND FUTURE WORK

The IDS is a technique which may be used for discovering the known and unknown intrusions before the attacker harms the devices of the network. In this paper, proposed Network intrusion has detected alert system by using a LSTM based on NSLKDD dataset.

For building a flexible and effective Network IDS by NSLKDD dataset. After preprocessing and normalize and feature selection by PCA. The proposed LSTM model for the detection of the attacks and threats. The LSTM model has been chosen by the comprehensive evaluation of their efficiency compared with the traditional machine learning types.

In addition, network-based features can be used in real-time and employed the suggested LSTM model for the detection of the attacks and intrusions. The current proposed model can perform better than previously implemented conventional machine learning types in network intrusion detection system.

Overall, the performance of training and testing by using LSTM architecture was good. It was observed that the IDS anomaly detection accuracy has shown a good percentage of detecting where the accuracy has reached more than 80 % while Detection rate reached to 94% and false alarm rate reached to 0.004%. Overall model performance has been good, particularly in the anomaly detection.

Current work can be extended in 3 directions where firstly, it is possible to apply the system on another intrusion dataset such as Kyoto, WSN-DS and CICIDS2017. Secondly, it may use another model to feature selection such as SVD and rough set and other. Thirdly, it tries to perform the offer approach online.

REFERENCES

[1] Ahmed M., Nasser Mahmood A., Hu J. (2016); A survey of network anomaly detection techniques, Journal of Network and Computer Applications, 60, 19–31, 2016.
[2] Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. (2014); Network anomaly detection: methods, systems and tools, Communications Surveys & Tutorials, IEEE, 16(1), 303–336,2014.
[3] Abd, D. H., & Obaida, T. H. (2016). A Robust Approach for Mixed Technique of Data Encryption Between DES and RC4 Algorithm. Journal of Kufa for Mathematics and Computer, 3(2), 48-54.
[4] Vinayakumar, R., et al. "Deep learning approach for intelligent intrusion detection system." IEEE Access 7 (2019): 41525-41550.

[5] P. Gogoi et al," Packet and flow based network intrusion dataset."Contemporary Computing". Springer Berlin Heidelberg, 2012. P 322-334.
[6] L. Li, Y. Yu, S. Bai, Y. Hou, and X. Chen, ''An effective two-step intrusion detection approach based on binary classification and k-NN,'' IEEE Access, vol. 6, pp. 12060–12073, 2018
[7] Yin, C.; Zhu, Y.; Fei, J.; He, X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access 2017, 5, 21954–21961.
[8] Farnaaz, N.; Jabbar, M.A. Random forest modeling for network intrusion detection system. Procedia Comput. Sci. 2016, 89, 213–217.
[9] Kim, G.; Lee, S.; Kim, S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Syst. Appl. 2014, 41, 1690–1700.
[10] Zaman, S.; Karray, F. Features selection for intrusion detection systems based on support vector machines. In Proceedings of the IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 10–13 January 2009; pp. 1–8.
[11] Kakavand, M.; Mustapha, N.; Mustapha, A.; Abdullah, M.T. Effective Dimensionality Reduction of Payload-Based Anomaly Detection in TMAD Model for HTTP Payload. KSII Trans. Internet Inf. Syst. 2016, 10, 3884–3910.
[12] Tahir, H.M.; Said, A.M.; Osman, N.H.; Zakaria, N.H.; Sabri, P.N.A.M.; Katuk, N. Oving K-means clustering using discretization technique in network intrusion detection system. In Proceedings of the 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 15–17 August 2016; pp. 248–252.
[13] Vinayakumar, R.; Soman, K.P.; Poornachandran, P. Applying convolutional neural network for network intrusion detection. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017; pp. 1222–1228.
[14] Canbay, Yavuz, and Seref Sagiroglu. "A hybrid method for intrusion detection." 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA). IEEE, 2015.
[15] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, ''A deep learning approach for network intrusion detection system,'' in Proc. 9th EAIInt. Conf.
[16] Jiang, Feng, et al. "Deep learning based multi-channel intelligent attack detection for data security." IEEE transactions on Sustainable Computing (2018).
[17] 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
[18] NSL-KDD dataset, obtainable by: https://www.unb.ca/cic/datasets/, September 2017
[19] KDD'99 datasets, Available on: http://kdd.ics.uci.edu/databases/kddcup 99/kddcup99.html, September, 2017.
[20] Abd, D. H., Sadiq, A. T., & Abbas, A. R. (2019, September). Classifying Political Arabic Articles Using Support Vector Machine with Different Feature Extraction. In International Conference on Applied Computing to Support Industry: Innovation and Technology (pp. 79-94). Springer, Cham.
[21] Abd, D. H., & Al-Mejibli, I. S. (2017, December). Monitoring System for Sickle Cell Disease Patients by Using Supervised Machine Learning. In *2017 Second Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)* (pp. 119-124). IEEE.
[22] Abd, D. H., Sadiq, A. T., & Abbas, A. R. (2020). PAAD: POLITICAL ARABIC ARTICLES DATASET FOR AUTOMATIC TEXT CATEGORIZATION. Iraqi Journal for Computers and Informatics, 46(1), 1-10.
[23] Ringnér, M. (2008). What is principal component analysis? Nature biotechnology, 26(3), 303-304.
[24] A. Graves, N. Jaitly, and A. Mohamed, "Hybrid speech recognition with deep bidirectional LSTM," in Automatic Speech Recognition and Understanding (ASRU), 2013 IEEE Workshop on. IEEE, 2013, pp. 273–278.
[25] Khalaf, M., Hussain, A. J., Keight, R., Al-Jumeily, D., Keenan, R., Chalmers, C., ... & Idowu, I. O. (2017, June). Recurrent neural network architectures for analysing biomedical data sets. In *2017 10th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 232-237). IEEE.
[26] Sak, H., Senior, A. W., & Beaufays, F. (2014). Long short-term memory recurrent neural network architectures for large scale acoustic modeling.
[27] Mehibs, Shawq Malik, and Soukaena Hassan Hashim. "Proposed network intrusion detection system in cloud environment based on back propagation neural network." Journal of University of Babylon for Pure and Applied Sciences 26.1 (2018): 29-40.