I. J. Computer Network and Information Security, **2019, 4, 19-25**
Published Online April 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.04.03

A Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection

Ahmed Iqbal, Shabib Aftab
Department of Computer Science, Virtual University of Pakistan
E-mail: ahmedeqbal@gmail.com, shabib.aftab@gmail.com

Received: 10 February 2019; Accepted: 24 February 2019; Published: 08 April 2019

***Abstract*—**Network security is an essential element in the day-to-day IT operations of nearly every organization in business. Securing a computer network means considering the threats and vulnerabilities and arrange the countermeasures. Network security threats are increasing rapidly and making wireless network and internet services unreliable and insecure. Intrusion Detection System plays a protective role in shielding a network from potential intrusions. In this research paper, Feed Forward Neural Network and Pattern Recognition Neural Network are designed and tested for the detection of various attacks by using modified KDD Cup99 dataset. In our proposed models, Bayesian Regularization and Scaled Conjugate Gradient, training functions are used to train the Artificial Neural Networks. Various performance measures such as Accuracy, MCC, R-squared, MSE, DR, FAR and AROC are used to evaluate the performance of proposed Neural Network Models. The results have shown that both the models have outperformed each other in different performance measures on different attack detections.

***Index Terms*—**Intrusion detection, Security, Anomaly detection, Intrusion Detection System, NSL-KDD, Neural Networks.

I. Introduction

In computer networks, an intrusion means to steal, alter, destroy or gain access to or make unauthorized use of a network system [1]. With the phenomenal growth of internet technology, network security has become a critical part of information security. Information Security is the basic concern of computing because many types of attacks are increasing day by day. Therefore, it is essential for network administrators to detect these kinds of attacks before they can occur. Many techniques and frameworks have been proposed for network instruction detection by providing high-speed intrusion detection mechanism. An Intrusion Detection System (IDS) is a mechanism to detect and prevent intrusive activities. It is considered a significant part in any information system which defends the network from any kind of potential intrusions. Usually the IDS do no not practically perform any action against attackers to prevent the attack; its main feature is to send an alert request to the network administrator that there is a suspected possible intrusion. Therefore, we can say that IDSs are proactive systems rather than a reactive system [2]. There are two different types of intrusion detection mechanism: 1) host-based, 2) network based. Each kind has different methods to defend and secure the network data, and each of them has its own pros and cons [3]. The host-based intrusion detection system examines the internal data of the computer network, while network-based instruction detection system examines data transmission between different computer networks [4]. Majority of researchers have recommended the use of KDD Cup99 dataset to predict network attacks. Most of the proposed methods failed to ensure high performance in detection rate. Some researchers have used all 41 available features of this dataset for detection which could lead to misclassification and also require much time to build the model [5]. On the other hand some of the researchers have selected the optimum subsets of features using feature selection techniques to improve the performance. This paper compares Pattern Recognition and Feed-Forward Neural network on intrusion detection and explores that which model delivers excellent results in term of Accuracy, MCC, R-squared, MSE, DR, FAR and AROC. The remaining paper is organized as follows: Section II presents the related work. Section III and IV presents the used KDD dataset and share some details of different intrusion attacks respectively. Section V presents Artificial Neural Network model. Section VI discusses various performance measures, used to evaluate the proposed model. The experimental results are presented in section VII. Conclusion is described in section VIII.

II. Related Works

Many researchers have been working on classification models using machine learning techniques in many areas such as sentiment classification [6,7,8,9,10,11] Rainfall predication [12,13] and Network instruction detection [14,15,16,17,18,19,20,21]. Some of the studies which have contributed in intrusion detection systems are discussed here. In [14] a mutual info-based algorithm is proposed and analytically chosen as the best feature for the classifications. The proposed algorithm can also parse a linear and nonlinear dependent data features. The result shows that the algorithm shares few other important features for LSSVM-IDS to get better accuracy results and low computation cost as compared to previous methods. Researchers in [15] reviewed different vulnerabilities in cloud computing systems and presented a collective instruction detection system to improve the privacy and security of the big data. Researchers in [16] presented a T-IDS, built on a novel randomized data portioned learning approach; it consists of a compact network feature selection technique, feature sets, and multiple randomized meta-learning techniques. This presented approach has successfully gained 99 percent accuracy and 21 second training time on botnet dataset. In [17], the research objective is to decrease the duration of active-time of the instruction detection system without adjusting their effectiveness. For validation, they proposed a model to reflect the interaction between intrusion detection systems as a multiplayer cooperative game where few players are practically conflicting, and some have feasible cooperative goals. [18] proposed a framework comprising of access control detection, protocol whitelisting, and multi-parameter-based detection. The SCADA-specific instruction detection system is applied, and results are validated by permanent and realistic cyber-physical test-bed and data from real 500kV smart substation. Researchers in [19] proposed an approach on how traffic can be distributed to multiple IDS in order to improve prediction the of network intrusions as well as to balance the load. The clustering-based approach is presented, which distribute flows reported by the routing information and flow data rate. Many experiments show that the presented scheme quickly detects attacks and deliver a better balance of traffic loads. In [20], researchers presented an IDS Internet of Things approach by using a suppressed fuzzy clustering-based algorithm and PCA scheme. The results show that as compared to past methods, this method generates better results. Researchers in [21] presented Spark-Chi-SVM scheme for the intrusion detection. The Researchers has adopted ChiSqSelector for the feature selection and developed an IDS technique by applying SVM based classifier on Apache Spark Big Data platform. The result shows that Spark-Chi-SVM approach delivers better performance and decrease training time for the Big data. Researchers in [22] proposed a new hybrid model that can be used to estimate the intrusion scope threshold degree based on the network transaction data's optimal features that were made available for training According to results the presented technique showed 99.81% and 98.56% results for the binary class and multi-class datasets respectively.

III. KDD CUP 1999 DATA

The KDD dataset is shared by MIT Lincoln Lab, and is widely used by many researchers during the past few years [23]. The experimental dataset used in our research work is a modified version of the KDD CUP99 data [40]. We have used four datasets (one for each attack type). Two types of datasets for each attack are available (1: with feature selection and 2: without feature selection). We have selected the normal dataset (without feature selection) and merged training and test data into one single file for each attack type. The merged datasets used in this research is available at [41]. This dataset was also pre-processed by using feature-coding. Furthermore, categorical feature encoding was used to change the categories to numeric values, and nominal field will then be represented in numerical categories instead of text. Nominal file represents certain classes, e.g., TCP, ICMP, UDP or hostnames, etc. After the feature-coding process, data features are displayed in the table.

Table 1. KDD Dataset Description

Name of the files	Features Description
KDD_DDoS.csv	duration, src_bytes, dst_bytes, land, wrong_fragment, urgent, hot, num_failed_logins, logged_in, num_compromised, root_shell, su_attempted, num_root, num_file_creations, num_shells, num_access_files, num_outbound_cmds, is_host_login, is_guest_login,count, srv_count ,serror_rate, srv_serror_rate, rerror_rate, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate, dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_srv_serror_rate, dst_host_rerror_rate, dst_host_srv_rerror_rate, protocol_type,service,flag
KDD_Probe.csv	
KDD_R2L.csv	
KDD_U2R.csv	

The training and test dataset both consist of 41 features labeled as normal traffic or specific attack types. The labels or classes of KDD data are further divided into two categories which represent attack or no attack accordingly.

IV. TYPES OF INTRUSIONS

The KDD Cup 1999 modified dataset contains the following four attack classes (Table. 1):

A). Denial-of-service Attack

It was 1999 when a new kind of attack was discovered which is later known as Distributed Denial-of-service attack [24]. A substantial amount of commerce, educational and even government websites suffered from this attack. DDoS attacker attempts to flood the network and prevents the network traffic. Sometimes, the attacker tries to disrupt a particular individual from accessing a required service. Hackers mostly attack by using DDoS for anything ranging from pranks to revenge against some corporations to express their anger or political activism [25].

B). Probe Attack

Probing is another type of attack in which hackers mostly scan targeted network computers to trace out potential vulnerabilities and weaknesses that may later be useful to exploit in the hope of attacking or compromising the entire system. Generally, Probing attacks are used in machine learning or data mining, e.g., portsweep, mscan, saint, and nmap [26].

C). Remote to Local Attack

In Remote to local attacks, the attacker tries to get access on the computers without having any account Remote to local intrusions are considered one of the most difficult attacks to detect in the network because they involve network level and host level features. So, diverse knowledge and technique are required to detect R2L attacks in the network [27].

D). User to Root Attack

The User to Root attack mostly requires semantic information that is critical to capture at early stages. Mostly, these types of attacks targeted the content-based applications. In U2R attacks, the attacker begins with access privilege of normal user and later become a super user or administrator to exploit the vulnerability of the network system [28].

V. Artificial Neural Network Model

The Artificial Neural Network is an interconnected set of units or neurons that use computational model for information-processing. A simple Neural Network contains three-layers; the first layer is known as an input layer of neurons, followed by the middle layer, and finally with outputs from the final layer of neurons. Artificial Neural Network can learn rapidly from experiences as well as from complex nonlinear problems [29]. Recently, many artificial network models have been reported as an effective way to detect intrusion in computer networks. In this research paper, we have proposed Feed-forward and Pattern recognition Neural network models for intrusion detection in the computer network.

A). Feed-Forward Network

The Feed-Forward network consists of multi-layered neurons. The first layer of neural network consists of neurons, having extremely applied input signals. Other layers receive their inputs only from their previous layer of network along with one bias signal source. Feed-Forward Network can be used in various problems, such as ECG abnormality detection, speech recognition, sentiment classification, balancing task, sensor signal processing, plant control etc. However, feed forward tasks are further divided into two classes: function approximation and pattern classification. In this research, we will primarily concentrate on pattern classification [30].

B). Pattern Recognition

Pattern recognition is considered as one of the hot research areas in machine learning domain. Mostly, Pattern Recognition Neural Networks are used for handwritten character recognition and image classification. The Pattern recognition neural networks are similar to feedforward ANN that can be train to classify inputs data according to their target labels [31]. In Matlab, The target data for these types of neural network should contain vectors of all zero values except for one in element i, where i is the actual class they are representing.

C). Back Propagation Algorithm

Back Propagation Algorithm is one of the highly adopted learning methods for Artificial Neural Network. Back Propagation refers to the broad family of Neural Networks, where the architecture consists of multiple interconnected sets of layers. Back Propagation is supervised learning algorithm for training an ANN that attempts to reduce the errors gradually [32]. For performance comparison, mostly MSE and Cross-Entropy measured are used. The two frequently adopted learning functions of the Backpropagation algorithm are discussed below.

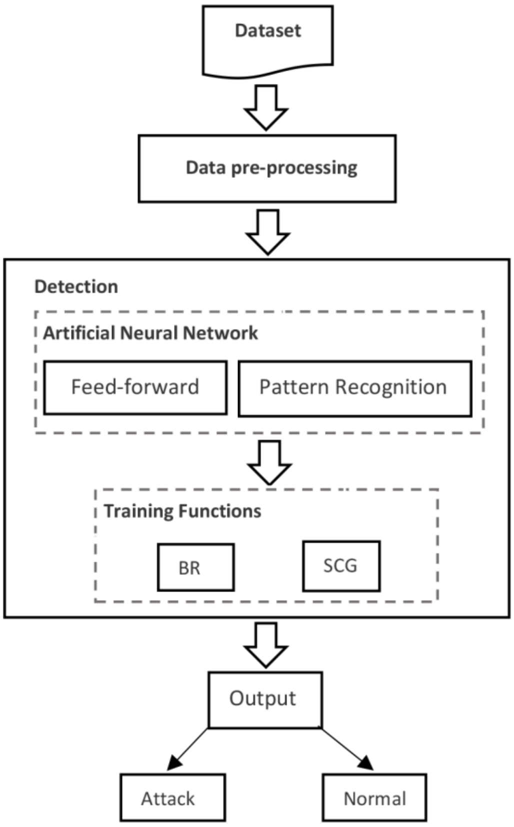

Fig.1. Proposed Model for Network Intrusion Detection

a) Bayesian Regularization

In this research, a Feed-Forward Neural Network is trained by using Bayesian Regularization function. BR algorithm works similarly to Levenberg Marquardt optimization in a sense that it minimizes squared errors and weights and finds out the optimal combination so that Neural Network can outperform [33]. In most of the problems, Bayesian Regularization training function gives more accurate results when compared to other training algorithms.

b) Scaled Conjugate Gradient

In our proposed model, Pattern Recognition Neural Network is trained by Scaled Conjugate Gradient training function. Scaled Conjugate Gradient training algorithm is using step size scaling mechanism; this technique reduces time consumption and line search per learning iteration. Most researchers agree that the Conjugate Gradient Method is a well-suited training function to deal with large scale problems in an efficient way [34].

VI. Performance Metrics

This research used many accuracy measures to evaluate the performance of the used ANN models which are discussed as follows.

R-squared (R^2) is known as the coefficient of determination. It is a statistical measure to overview that how close enough the data is to be fitted within the regression line. The R-squared value of the test data is measured to determine how much the used technique fits the data. R-squared > 0.9 is treated as good fit [35].

Mean Squared Error (MSE) is the average of squared error that is used as loss function for least squares regressions. MSE is the sum of the squared difference among predicated and actual targets, divided by the number of data points [36].

$$MSE = \frac{\sum (t_{i-} o_i)^2}{n} \tag{1}$$

The Area Under Curve (AUC) is mostly measured to compare different ROC curves. The high value of AUC indicates that the classifier is producing more accurate predictions. AUC provides an aggregate measure of performance across all possible classification thresholds. AROC is the area under ROC curve. It is a single number summary of the performance [37].

Detection Rate (DR) indicates the ratio among total number of intrusions detected by the system (True Positive) to a total number of intrusions present in the dataset [38].

$$DR = \frac{TP}{TP + FN} \tag{2}$$

False Alarm Rate (FAR) is the measurement of performance which indicates the rate of samples misclassified and a total number of typical association show in the dataset.

$$FAR = \frac{FP}{TN + FP} \tag{3}$$

Mathew's Correlation Coefficient (MCC) is also considered as one of the widely used performance measure metric. It is defined as the ratio between the observed and predicted binary classifications [39].

$$MCC = \frac{TN * TP - FN * FP}{\sqrt{(FP + TP)(FN + TP)(TN + FP)(TN + FN)}} \tag{4}$$

In the confusion matrix, Accuracy is the measurement rate of correct classifications. Accuracy is calculated by taking the ratio of correct prediction to total number of predictions. Accuracy can be expressed as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

VII. RESULTS & Discussion

The purpose of this research is to analyze the performance of Feed Forward Artificial Neural Network FFANN and Pattern Recognition Artificial Neural Network (PRANN) on the detection of various network attacks. All experiments are conducted in MATLAB 2018. In Feed-forward and Pattern Recognition neural network, 10 neurons were used with a single hidden layer. The input layer of the Artificial Network has a total number of neurons equal to a total number of features or attributes in a given dataset. In the final output layer of the ANN, two neurons are used which belong to the class as attack or no attack modules accordingly. The Feed-Forward Neural Network is trained by using Bayesian Regularization training function, and Pattern Recognition Neural Network is trained by Scaled Conjugate Gradient training function. The dataset is divided into three different parts: 70% of training data, 15% of validation data, and 15% of test dataset. The experiential results of proposed approaches are presented in Table 2 in terms of Accuracy, MCC, R-squared, and MSE for U2R attacks.

Table 2. Results for Root Attack (U2R)

Model	Accuracy	MCC	R-squared	MSE
FFANN	99.8356	0.9967	0.9902	0.0050
PRANN	99.6712	0.9934	0.9941	0.0029

The highest Accuracy and MCC are obtained by FFANN Model. However, PRANN outperformed in terms of R-squared and MSE.

Table 3. Results for Denial of Service Attack (DoS)

Model	Accuracy	MCC	R-squared	MSE
FFANN	99.7429	0.9949	0.9927	0.0036
PRANN	98.7952	0.9759	0.9807	0.0096

Table 3 shows the results obtained from both the models (FFANN, PRANN) regarding the detection of Denial of Service Attack (DoS). FFANN outperformed in all measured (Accuracy, MCC, R-squared, and MSE).

Table 4. Results for Probing Attack

Model	Accuracy	MCC	R-squared	MSE
FFANN	98.8345	0.9767	0.9790	0.0104
PRANN	98.9232	0.9785	0.9826	0.0086

Table 4 shows the results obtained from both models (FFANN, PRANN) and reflects that PRANN performed better in all measures.

Table 5. Results for Remote to Local Attack (R2L)

Model	Accuracy	MCC	R-squared	MSE
FFANN	98.0742	0.9615	0.9673	0.0161
PRANN	96.6225	0.9325	0.9474	0.0256

Table 5 shows the results obtained from both models and shows that the highest Accuracy, MCC, R-squared, and MSE is obtained by FFANN Model.

A). DR Comparison Results

Fig 2 shows the DR measures of classifiers used in this research. With FFANN, we got highest with 0.9987 score for U2R and lowest with 0.9777 for R2L. However, in the PRANN model, highest DR is recorded with score 0.9960 for U2R and lowest 0.9668 for R2L.

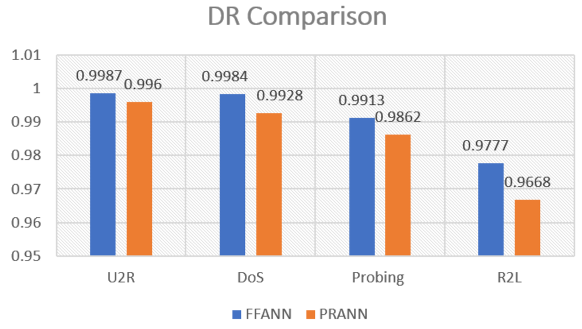

Fig.2. Comparison of the DR Results

B). FAR Comparison Results

Fig 3 shows the FAR measures of each classifier used in this research. PRANN reflected the highest score with 0.0356 for R2L and the lowest with 0.0033 for U2R. In the FFANN model, highest FAR is recorded with 0.0197 score for R2L and lowest with 0.0018 score for U2R.

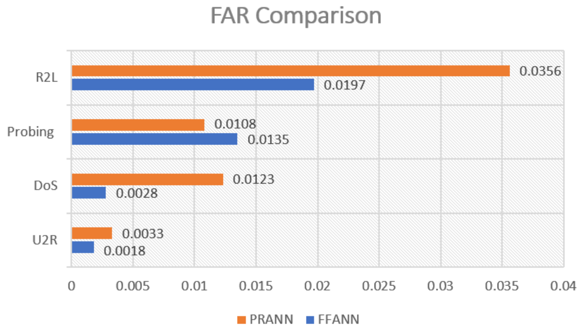

Fig.3. Comparison of the FAR Results

C). AROC Comparison Results

Fig 4 shows the areas under ROC curves of both the classifiers used in this research. The highest score with PRANN is 0.9999 for U2R and lowest score is 0.9953 for R2L. By using FFANN model, highest AROC sore 0.9998 is recorded for DoS and lowest score 0.9977 is recorded for R2L.

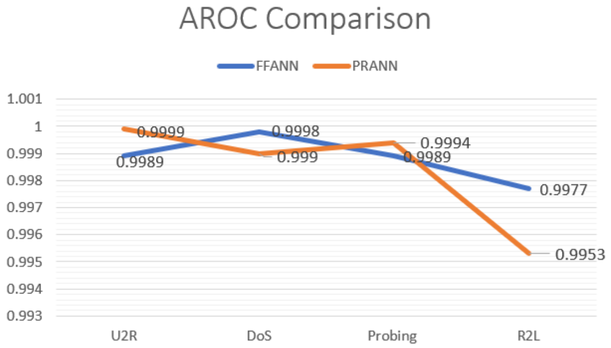

Fig.4. Comparison of the AROC

VIII. Conclusion

Network security is a wide term to define. In its broader sense, we can say that it means to protect the confidential information or data which is stored on the network. Many organizations want to detect the intrusion in the network before they can be under attacked or to experience the loss of confidential data. To help in this case, various intrusion detection systems have been proposed and developed along with a large number of published literatures. This research paper proposes Feed-Forward and Pattern Recognition Neural Network models with Bayesian Regularization and Scaled Conjugate Gradient training functions to detect intrusion in the network. Both networks out performed each other in different performance measures on different intrusion attacks. This research can be used as a baseline for further comparisons as well as for future innovations for performance improvements. Both the used networks should be further tuned and used for more diverse intrusion datasets.

References

[1] R. Tewatia, A. Mishra, “Introduction to Intrusion Detection System: Review,” Int. J. Sci. Technol. Res., vol. 4, no. 05, MAY 2015.

[2] S. Mukkamala, G. Janoski, A. Sung, “Intrusion Detection: Support Vector Machines and Neural Networks,” IEEE Xplore, 2002.

[3] R. Beghdad, “Efficient deterministic method for detecting new U2R attacks,” Comput. Commun., vol. 32, no. 6, pp. 1104–1110, 2009.

[4] M. Sazzadul Hoque, “An Implementation of Intrusion Detection System Using Genetic Algorithm,” Int. J. Netw. Secur. Its Appl., vol. 4, no. 2, pp. 109–120, 2012.

[5] J. McHugh, “Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory,” ACM Trans. Inf. Syst. Secur., vol. 3, no. 4, pp. 262–294, 2000.

[6] M. Ahmad, S. Aftab, and I. Ali, “Sentiment Analysis of Tweets using SVM,” Int. J. Comput. Appl., vol. 177, no. 5,

pp. 25–29, 2017.

[7] M. Ahmad, S. Aftab, I. Ali, and N. Hameed, “Hybrid Tools and Techniques for Sentiment Analysis: A Review,” Int. J. Multidiscip. Sci. Eng., vol. 8, no. 3, 2017

[8] M. Ahmad and S. Aftab, “Analyzing the Performance of SVM for Polarity Detection with Different Datasets,” Int. J. Mod. Educ. Comput. Sci., vol. 9, no. 10, pp. 29–36, 2017.

[9] M. Ahmad, S. Aftab, M. Salman, N. Hameed, I. Ali, and Z. Nawaz, “SVM Optimization for Sentiment Analysis,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 4, 2018.

[10] M. Ahmad, S. Aftab, and S. S. Muhammad, “Machine Learning Techniques for Sentiment Analysis: A Review,” Int. J. Multidiscip. Sci. Eng., vol. 8, no. 3, p. 27, 2017.

[11] M. Ahmad, S. Aftab, M. Salman, and N. Hameed, “Sentiment Analysis using SVM: A Systematic Literature Review,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 2, 2018.

[12] S. Aftab, M. Ahmad, N. Hameed, M. Salman, I. Ali, and Z. Nawaz, “Rainfall Prediction in Lahore City using Data Mining Techniques,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 4, 2018.

[13] S. Aftab, M. Ahmad, N. Hameed, M. Salman, I. Ali, and Z. Nawaz, “Rainfall Prediction using Data Mining Techniques: A Systematic Literature Review,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 5, 2018.

[14] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, “Building an intrusion detection system using a filter-based feature selection algorithm,” IEEE Trans. Comput., vol. 65, no. 10, pp. 2986–2998, 2016.

[15] Z. Tan et al., “Enhancing big data security with collaborative intrusion detection,” IEEE Cloud Comput., vol. 1, no. 3, pp. 27–33, 2014.

[16] O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo, S. Muhaidat, K. Taha, and K. Kim, “Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection,” IEEE Trans. Cybern., vol. 46, no. 8, pp. 1796–1806, 2016.

[17] N. Marchang, R. Datta, and S. K. Das, “A novel approach for efficient usage of intrusion detection system in mobile Ad Hoc networks,” IEEE Trans. Veh. Technol., vol. 66, no. 2, pp. 1684–1695, 2017.

[18] Y. Yang, H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin, and S. Sezer, “Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks,” IEEE Trans. Power Deliv., vol. 32, no. 2, pp. 1068–1078, 2017.

[19] T. Ha, S. Yoon, A. C. Risdianto, J. W. Kim, and H. Lim, “Suspicious flow forwarding for multiple intrusion detection systems on software-defined networks,” IEEE Netw., vol. 30, no. 6, pp. 22–27, 2016.

[20] X. Z. and X. W. Liqun Liu, Bing Xu2*, “An intrusion detection method for internet of things based on suppressed fuzzy clustering,” J. Wirel. Commun. Netw., 2018.

[21] S. M. Othman, F. M. Ba-Alwi, N. T. Alsohybe, and A. Y. Al-Hashida, “Intrusion detection model using machine learning algorithm on Big Data environment,” J. Big Data, vol. 5, no. 1, 2018.

[22] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, “Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model,” J. Comput. Sci., vol. 25, pp. 152–160, 2018.

[23] “KDD Cup 1999 Data.” [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. [Accessed: 19-Jan-2019].

[24] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, “A survey of distributed denial-of-service attack, prevention, and mitigation techniques,” Int. J. Distrib. Sens. Networks, vol. 13, no. 12, 2017.

[25] M. S. Galina Mikhaylova, “The ‘Anonymous’ Movement: Hacktivism as an Emerging Form of Political Participation,” Graduate Council of Texas State University, 2014.

[26] S. Paliwal and R. Gupta, “Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm,” Int. J. Comput. Appl., vol. 60, no. 19, pp. 975–8887, 2012.

[27] M. Sabhnani and G. Serpen, “KDD feature set complaint heuristic rules for R2L attack detection,” Proc. Int. Conf. Secur. Manag., vol. 1, pp. 310–316, 2003.

[28] F. Mozneb and A. Farzan, “The Use of Intelligent Algorithms to Detect Attacks In,” vol. 3, no. 9, pp. 579–584, 2014.

[29] V. Sze, Y. Chen, T. Yang, and J. Emer, “Efficient processing of deep neural networks: A tutorial and survey”, Mar. 2017.

[30] O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. E. Mohamed, and H. Arshad, “State-of-the-art in artificial neural network applications: A survey,” Heliyon, vol. 4, no. 11. Elsevier Ltd, p. e00938, 2018.

[31] M. S. Piotr Gaj, Andrzej Kwiecień, Computer Networks: 24th International Conference, CN 2017, Lądek Zdrój, Poland, June 20–23, 2017, Proceedings. Springer, 2017.

[32] A.K. Jain, J. Mao, and K.M. Mohiuddin, ªArtificial Neural Networks: A Tutorial, Computer, pp. 31-44, Mar. 1996.

[33] K. Gopalakrishnan, “Effect of training algorithms on neural networks aided pavement diagnosis,” Int. J. Eng. Sci. …, vol. 2, no. 2, pp. 83–92, 2010.

[34] M. Fodslette Møller, “A scaled conjugate gradient algorithm for fast supervised learning,” Neural Networks, vol. 6, pp. 525–533, 1993.

[35] J. Bourquin, H. Schmidli, P. Van Hoogevest, and H. Leuenberger, “Comparison of artificial neural networks (ANN) with classical modelling techniques using different experimental designs and data from a galenical study on a solid dosage form,” Eur. J. Pharm. Sci., vol. 6, no. 4, pp. 287–300, 1998.

[36] K. Das, J. Jiang, and J. N. K. Rao, “Mean squared error of empirical predictor,” Ann. Stat., vol. 32, no. 2, pp. 818–840, 2004.

[37] T. Fawcett, “An introduction to ROC analysis,” Pattern Recognit. Lett., vol. 27, no. 8, pp. 861–874, 2006.

[38] M. A. Jabbar, R. Aluvalu, and S. S. Reddy, “RFAODE: A Novel Ensemble Intrusion Detection System,” Procedia Comput. Sci., vol. 115, pp. 226–234, 2017.

[39] S. Boughorbel, F. Jarray, and M. El-Anbari, “Optimal classifier for imbalanced data using Matthews Correlation Coefficient metric,” PLoS One, vol. 12, no. 6, pp. 1–17, 2017.

[40] “NSLKDD-Dataset.” [Online]. Available: https://github.com/InitRoot/NSLKDD-Dataset. [Accessed: 02-April-2019].

[41] “Modified NSLKDD-Dataset.” [Online]. Available: https://github.com/ahmedeqbal/Modified-NSL-KDD-Dataset-1. [Accessed: 02-Apr-2019].

Authors’ Profiles

Ahmed Iqbal is a student of MS Computer Science with the specialization of Software engineering in Virtual University of Pakistan. He received the degree, Master of Information Technology (MIT) from Virtual University of

Pakistan in 2016. His research interest includes Software Engineering and Data Mining.

Shabib Aftab received MS Degree in Computer Sciences from COMSATS Institute of Information Technology Lahore, Pakistan. He is serving as Lecturer Computer Sciences at Virtual University of Pakistan. His research areas include Data Mining and Software Process Improvement.

How to cite this paper: Ahmed Iqbal, Shabib Aftab,"A Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.4, pp.19-25, 2019.DOI: 10.5815/ijcnis.2019.04.03