ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse276952020.pdf
https://doi.org/10.30534/ijatcse/2020/276952020

A cascading layered approach for Intrusion Detection to improve detection accuracy of Major and Minor Attacks

Utpal Shrivastava[1], Neelam Sharma[2]
[1]Banasthali Vidyapith, Banasthali, India, utpalshrivastava@gmail.com
[2]Banasthali Vidyapith, Banasthali, India, sharmaneelam27@gmail.com

ABSTRACT

The growth of computer network for inter communication and data sharing has also raised the challenge of security of data over network. There are many threat or attacks in network that tries to privacy theft of data over network. Intrusion Detection System (IDS) is helpful to protect network form attacks. The attacks over network is divided into four categories i.e. User-to-Root (U2R), Root-to-User (R2L), Prob and Denial-of-Service (DoS). In this paper, a cascading layered based approach is follow to make an IDS. The approach is followed to improve the detection rate of all categories of attacks. Feature selection for Prob & DoS attacks and U2R & R2L attacks is done. An Artificial Neural Network (ANN) is used to improve the detection accuracy of U2R and R2L attacks. The training data for minor attacks is resampled to detect any novel attacks. The proposed approach gives a very good results.

Key words: Intrusion detection, Feature selection, Pattern matching, Security.

1. INTRODUCTION

The computer network is exponentially growing year by year. The world is dependent on these network for their intercommunication and data sharing. This make an opportunity for the users trying to extract data for these network by illegal means. Such attempts are protected with the help of Intrusion detection system. The network architecture is vulnerable to different types of attacks with its own aims. The Intrusion Detection System (IDS) is a way of detecting any known or unknown vulnerability in network. The system continuously monitor all network traffic for any suspicious network traffic that could be a threat. If any unusual network pattern is found then an alert is raised to check the possibility of attack. The threat can be of two types misuse and anomaly. Misuse is the case where such attack has already had occurred and their network pattern is known. Whereas the anomaly is the case where attack pattern or signature is not known. Consistent updating of the IDS database is needed for the latest attack patterns known on the network. There are two host-based and network-based IDS. In host-based IDS, the data traffic for host to network and from network to host is monitored to detect potential threat or attacks. The IDS is put in network in network-based IDS, which analyses all data traffic activity to detect any potential attacks / threats. As follows, there could be four types of network attacks divided into two categories:

Major attacks

- DoS: Tries to block some particular kind of use of resources.
- Probe: Host information is collected..

Minor attacks

- U2R: its aim is to gain local access to the root rights of a host.
- R2L: Intended to gain sole rights from a distant location to the local host.

Network data traffic can be used to identify it pattern is matching to normal data traffic or attack data traffic. As the there are two categories of attack major and minor attack, Major attacks are very common in network and there data patter or signature is known, hence it's easy to find such attacks in network i.e Prob and DoS . Whereas the minor attacks are very rarely seen in the network, hence their data traffic pattern are not commonly seen i.e R2L and U2R. The detection rate of minor attacks are low in the network. Minor attack are uncommon in network but they are very harmful as these attacks tries to capture a host. Researchers proposed may models to improve the accuracy for minor attack detection but there is a lot of scope of further improving it.

2. RELATED WORK

Data security is a fundamental feature of any network. The Intrusion detections system play an important role in this. There are many work done by researchers to make any efficient IDS model. The researchers has proposed model with minimum number of features and on the under sampling of the attacks pattern in the dataset. Different machine learning algorithms are used to propose the model. In [1] author has proposed pattern search algorithm . The performance of Boyer-Moore algorithm and Rabin-Karp algorithm is checked. Author proposed a DNA encoding

methodology by taking all 41 features of the KDD cup dataset as nucleotide sequence. They compared there proposed technique with other existing exact string matching algorithms. The Author[2] has proposed IDS model based on artificial immune system. Negative and positive, are treated as antibodies. Simulation result shows a good result with 99.1 percent present to positive rate 1.9% false positive rate. Particle Swarm Optimization (PSO) is used for training the model. In [3] author has proposed a model for detecting new types of attacks based on the existing attack pattern. They have used a concept hierarchy generation (CHGL) to label attacks. The subset of codes clustering with CHGL helps to detect profiles of high concept levels to find more attacks. In [4]proposed a hybrid IDS using ensemble classifier. They worked on data and its feature to improve the detection rate of the overall system. In[5] author proposed an IDS model based on the SVM and genetic programming to improve the detection rate of the rare attacks. They got an accuracy of 90.72 % for R2L attacks and 88.24 % for the U2R attacks. In author proposed a layered approach where they had used a two tier architecture of IDS to improve True positive rate. They got a TP rate of 99%.In [6]authors has proposed IDS model based on Naïve Bayes classifier. The feature engineering is done to find the importance of features in dataset based on the attack categories. The got a recall rate of 80.8% for U2R attacks, 97% for R2L attacks, 98.8% for Probe attacks and 99.9% for DoS attacks. In [7]author proposed IDS model to improve the memory utilization and reduce the false positive rate of the overall system. An ensemble binary SVM model is proposed[8]. For feature extraction they have used PCA and LDA algorithms. Fuzzy based PCA is used to make IDS[9]. To classify K nearest neighbor is used. They got good results in detecting U2R and DoS attacks. In [10]author had done deep analysis of KDD Cup99 dataset. In [11] author has used a multiple convolution layer concept with softmax classifier. Their model is also able to detect anomaly attacks. A deep learning approach is used in [12] for matching attack patterns. NSL-KDD dataset is used to train the logistic classifier. In [13] author has used Deep neural network to propose their IDS model. They tested their model for different datasets.

3. NSL- KDD

NSL-KDD dataset[14] is an improved version of KDD 99 data set. KDD 99 dataset was having redundant records which is removed in test NSL-KDD dataset. Duplicate records from the train dataset is also removed. Different difficulty level of records are also considered in the NSL-KDD dataset. Each record in the dataset is of 100 bytes. NSL-KDD dataset is improved to get better classification rate in machine learning algorithms.

The dataset has four types of attacks DoS (Att_Type_1), Prob (Att_Type_2), U2R (Att_Type_3) and R2L (Att_Type_4). In addition to the records of these types of attacks there are also normal records in the dataset. The train dataset has total 125972 records. 67342 records are labeled as normal and remaining 58630 records are labeled as one of the attack types. In NSL- KDD dataset there are total 38 types of attacks. In the training set there are only 22 type attack labels i.e, imap, multihop, phf, spy, warezclient, buffer_overflow, warezmaster, perl, loadmodule, ipsweep, rootkit, ftp_write, guess_passwd, nmap, port sweep, back, land, Neptune, pod, smurf, teardrop, and satan. Att_Type_1 attacks are back, land, pod, Neptune, teardrop, and smurf. Att_Type_2 attacks are ipsweep, nmap, portsweep, and satan. Att_Type_3 attacks are loadmodule, buffer_overflow, rootkit, and Perl. Att_Type_4 attacks are guess_passwd, ftp_write, multihop, imap, phf, spy, warezmaster, and warezclient. Distribution of Att_Type_1 attacks is shown in Figure1, Att_Type_2 in Figure 2, Att_Type_3 in Figure 3 and Att_Type_4 in Figure 4.

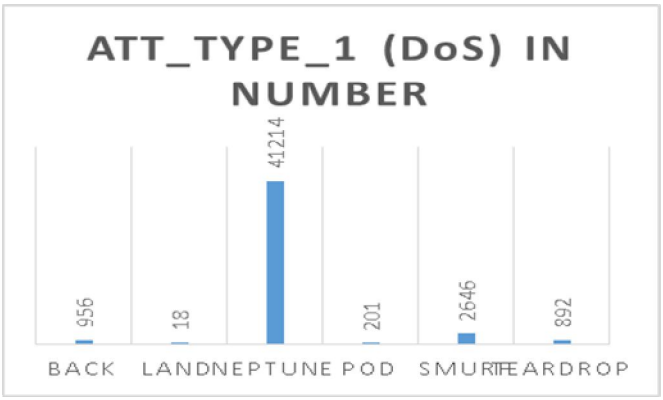

Figure 1: Distribution of DoS attacks in dataset.

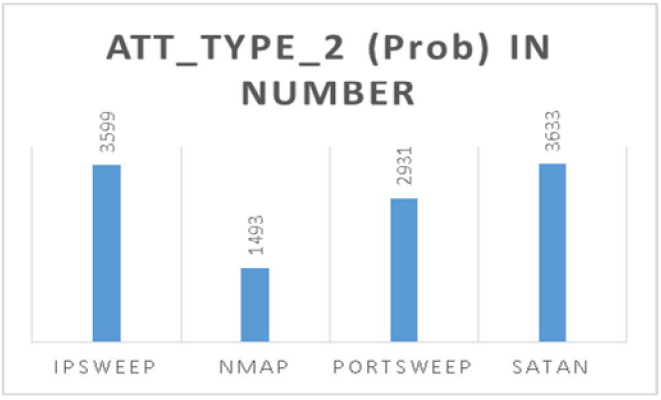

Figure 2: Distribution of Prob attacks in dataset.

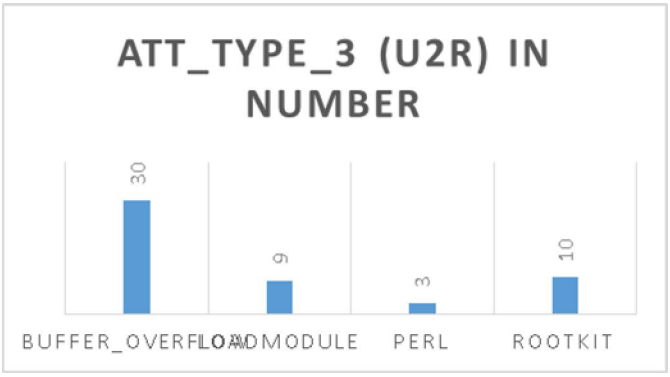

Figure 3: Distribution of U2R attacks in dataset.

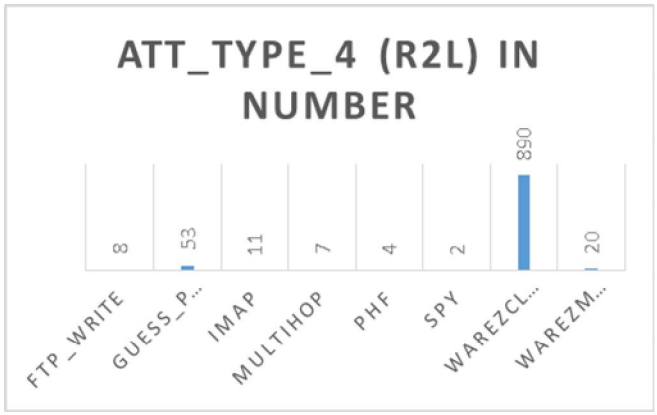

Figure 4: Distribution of R2L attacks in dataset.

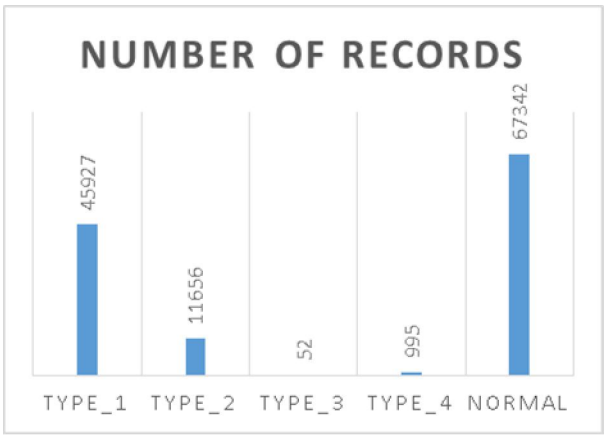

Figure 5: Number of recodes based on attack categories

The distribution of attacks and number of records in each categories is shown in the Figure 5. It can be observed form the figure 5 that Att_Type_1 and Att_Type_2 attack samples in the dataset is adequate. These attacks are also known as major attacks as it is commonly found in the network. Number of records for attacks Att_Type_3 and Att_Type_4 are very less compare to Att_Type_1 and Att_Type_2 attacks. These attacks are known as minor attacks or rare attacks. This types of attacks are rarely seen in network though these attacks are also very harmful threats in the network.
The test dataset of NSL-KDD has more label of attacks which is helpful to test a model for detecting unseen attacks.

4. FEATURE SELECTION

Feature selection is way to identify the most important features of a dataset. Features that contributes in identifying the attack types are selected to train and test a machine learning model. There are 42 features in the dataset. The 42th feature is label of the records as attack name or normal. The features in the dataset are numbered from Fe1 to Fe41 in the proposed work. Feature selection is done for two categories of attacks i.e. major attacks (Att_Type_1 and Att_Type_2) and minor attacks (Att_Type_3 and Att_Type_4). The dataset is divided into two parts one part of dataset has only major attacks named as major_dataset and other has only minor attacks named as minor_dataset. All attacks in the dataset is labeled by category of attack i.e. Att_Type_1, Att_Type_2, Att_Type_3 and Att_Type_4.

4.1 Major Dataset

The feature number Fe2, Fe3 and Fe4 is converted into numeric data type. Features Fe20 having zero variance is removed from the dataset. The cut off of 0.8 is taken and features Fe28, Fe33, Fe37, Fe25, Fe38 Fe27, Fe26, Fe40, Fe13 and Fe21 are found correlated. These features are also deleted from the dataset. To find the importance of features, Learning Vector Quantization (LVQ)[15] model is used. The importance of top 20 features are shown in Table 1 and Figure 6 show importance of all the features remaining in the dataset.

The observation of table 1 and figure 6 shows that feature can be further remove to reduce the dimensionality complexity of dataset. The 12 features with the importance greater than 0.80 is finally selected to train the model.

Table 1: ROC curve

Variable importance (ROC curve)			
Twenty most important features			
	Att_Type_1	Att_Type_2	normal
Fe5	0.9008	0.9492	0.9492
Fe29	0.9384	0.7268	0.9384
Fe23	0.9308	0.8218	0.9308
Fe6	0.9016	0.9157	0.9157
Fe34	0.9071	0.7334	0.9071
Fe4	0.907	0.6916	0.907
Fe30	0.9033	0.651	0.9033
Fe36	0.8731	0.8731	0.7925
Fe26	0.8681	0.8551	0.8681
Fe39	0.8651	0.8563	0.8651
Fe35	0.8579	0.7294	0.8579
Fe12	0.8447	0.8516	0.8516
Fe32	0.7764	0.7287	0.7764
Fe24	0.7055	0.7055	0.6178
Fe41	0.6437	0.6946	0.6946
Fe31	0.6759	0.6457	0.6759
Fe2	0.5992	0.6579	0.6579
Fe3	0.6399	0.5815	0.6399
Fe1	0.568	0.568	0.5587
Fe8	0.5119	0.5119	0.5119

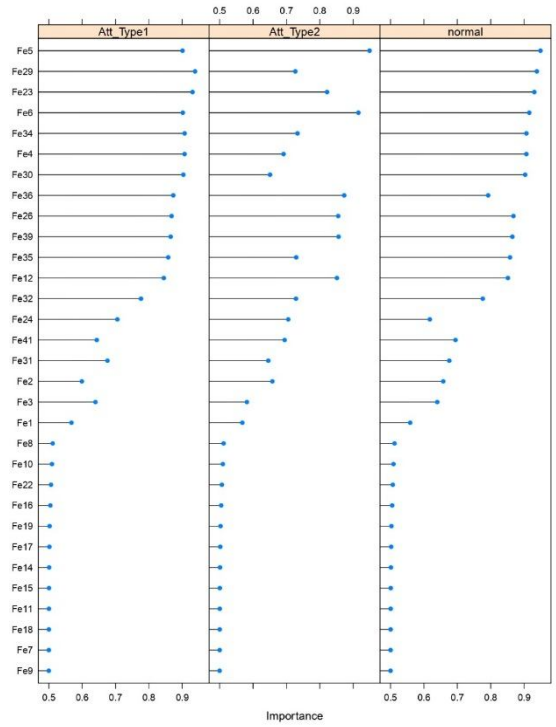

Figure 6: Importance of features

4.2 Minor Dataset

The feature number Fe2, Fe3, and Fe4 is converted into numeric data type. Features Fe8, Fe20, and Fe21 having zero variance is removed. The cut off 0.8 is taken and features "Fe4", "Fe27", "Fe28", "Fe40", "Fe24", "Fe16", "Fe22" "Fe25" are found correlated. These features are also removed from the dataset. Learning Vector Quantization (LVQ)[15] model is also used for minor dataset to find importance of the features in the dataset. The Table 2 show the importance of top 20 features in the dataset and Figure 7 show the importance of all the features in the dataset as per its categories.

Table 2: ROC curve (minor dataset)

Variable importance(ROC curve)			
Twenty most important features			
	Att_Type_3	Att_Type_4	normal
Fe33	0.947	0.8854	0.947
Fe6	0.8462	0.8462	0.7505
Fe3	0.844	0.844	0.7543
Fe32	0.8283	0.7014	0.8283
Fe1	0.8125	0.7254	0.8125
Fe23	0.7621	0.7859	0.7859
Fe36	0.7856	0.7162	0.7856
Fe5	0.592	0.7643	0.7643
Fe10	0.7577	0.7044	0.7577
Fe14	0.7489	0.747	0.7489
Fe17	0.7189	0.7165	0.7189
Fe13	0.7187	0.7187	0.7177
Fe31	0.6811	0.666	0.6811
Fe37	0.6383	0.6383	0.6258
Fe38	0.6065	0.6065	0.5635
Fe12	0.5881	0.6025	0.6025
Fe2	0.5552	0.5835	0.5835
Fe35	0.5778	0.5737	0.5778
Fe39	0.571	0.571	0.5445
Fe29	0.5542	0.5542	0.5278

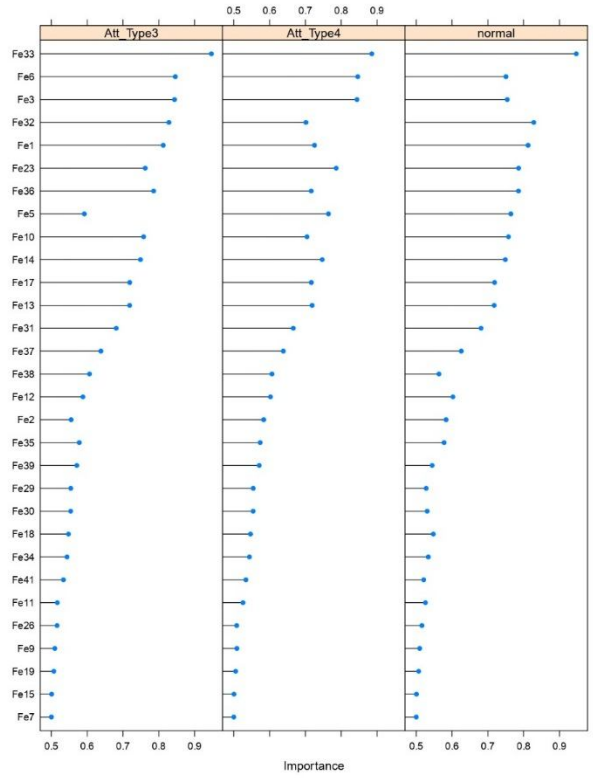

Figure 7: Importance of features base on LVQ for minor dataset

The minimum set of features are also selected for minor dataset as done for major dataset. The adaboosting algorithm is used on different set of feature set based on its importance. Based on the results the minimum number of features are selected for the minor dataset. Output obtained with different number of features set is shown in Table 3.

The 20 feature set of Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14, Fe17, Fe13, Fe31, Fe37, Fe38, Fe12, Fe2, Fe35, Fe39, Fe29 has an accuracy of 0.9963768 with precision and recall rate of Att_type_3 and Att_type_4 is 0.8 , 1 , 1 and 0.969697. For 16 feature set Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14, Fe17, Fe13, Fe31, Fe37, Fe38, Fe12 the accuracy obtained is same as of 20 feature set.

Table 3: Adaboosting model accuracy for different feature selected (minor dataset)

Features Selected	precision		recall		accuracy
	Att_Type_3	Att_Type_4	Att_Type_3	Att_Type_4	
Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14, Fe17, Fe13, Fe31, Fe37, Fe38, Fe12, Fe2, Fe35, Fe39, Fe29	0.8	1	0.8	0.969	0.9963768
Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14, Fe17, Fe13, Fe31, Fe37, Fe38, Fe12	1	1	0.8	0.969697	0.9963768
Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14, Fe17, Fe13	0.8	1	0.8	0.969697	0.996377
Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14	1	1	0.8	0.969697	0.996377
Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5	1	0.989690 7	0.8	0.969697	0.995471
Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36	1	0.968085 1	0.8	0.9191919	0.9891304

Set of 12 features set “Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14, Fe17, Fe13”, set of 10 features set “Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5, Fe10, Fe14” and set of 8 feature set of “Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, Fe5” have nearly same accuracy i.e. 0.996377 and 0.995471. The accuracy decreases when set of seven features “Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36” is taken in consideration with an accuracy of 0.9891304. After the analysis of the output received the final feature selected are Fe33, Fe6, Fe3, Fe32, Fe1, Fe23, Fe36, and Fe5. The accuracy of the model is improved using different machine learning models.

5. LAYERED APPROACH

A layered approach is followed (Figure 8) to improve the detection rate of rare attacks. The proposed model has two layers one layer is used for detecting major attacks and other layer is used to detect minor attacks.

In the proposed model NSL-KDD dataset is used to train the model. The dataset is divided in to parts based on the attack category. Major Dataset has the attack pattern of major attacks with normal data and Minor Dataset has the attack pattern of minor attacks with normal data. The feature extraction is done on the both dataset one by one. The reduced dataset with selected feature is given as input for training the model. Level II is trained for the major attacks. Level I is trained for the minor attacks. Network traffic with selected features for major attacks are given as input to Level II.

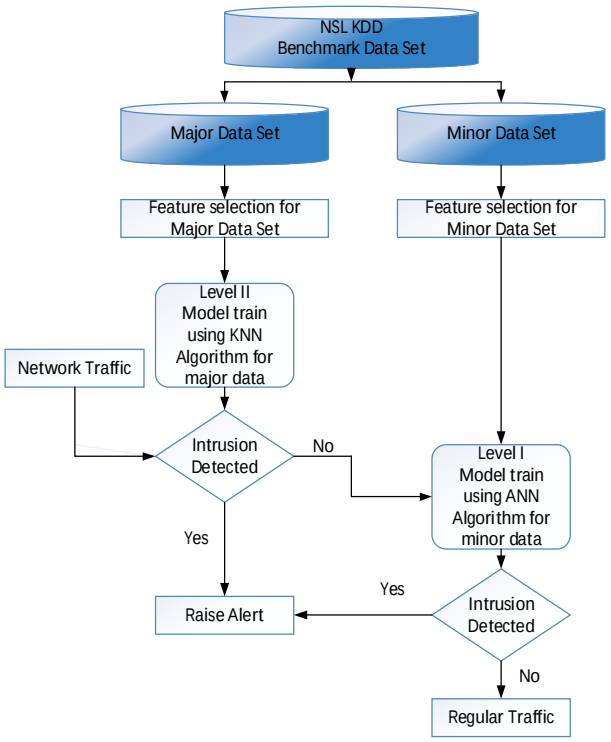

Figure 8: Proposed Approach

Table 4: Procedure

Algorithm 1:Procedure

Task 1: *NSL-KDD Dataset for training the model.*

Task 2*: Preparing two dataset, one for major attacks (Major Dataset) and other for minor attacks(Minor dataset)*

Task 3: *Feature selection is done for Major Dataset and Minor Dataset separately.*

Task 4: *Both Dataset is divided in ratio of 9:1 for training and testing of the model.*

Task 5: *For minor attack at level I Artificial neural network machine learning algorithm is used to train model and Major attack model is trained using Random forest at label II.*

Task 6: *Data traffic is given as input at level II, and checked for major attacks. If not found then the traffic is further passed through level I to check for minor attacks, if intrusion found an alert is raised.*

Task 7: *The network traffic is further checked to confirm attack on alert raised else treated as normal data traffic.*

An alert is raised on the occurrence of attack pattern. Then the network traffic with selected features for minor attack is given as input to the Level I. If intrusion is detected then alert is raised. If no alert is raised at Level II and Level I then network traffic is treated as regular traffic. Procedure is shown in Figure 8 and Table4.

In Level II of the proposed approach for major data different machine learning algorithms are tested for accuracy and the best observed accuracy is selected. Machine learning

algorithms Random Forest, KNN, J48, SVM and CART accuracy obtained is shown in the Table 5.

Table 5: Models accuracy for major attacks

Trained by Major Dataset			
Machine learning models	Accuracy in %		
	Att_Type3	Att_Type4	normal
Random Forest	99.686	99.795	99.21
KNN	96.563	97.657	99.01
J48	87.546	88.361	98.23
SVM	98.767	98.08	99.03
CART	91.466	95.346	98.89

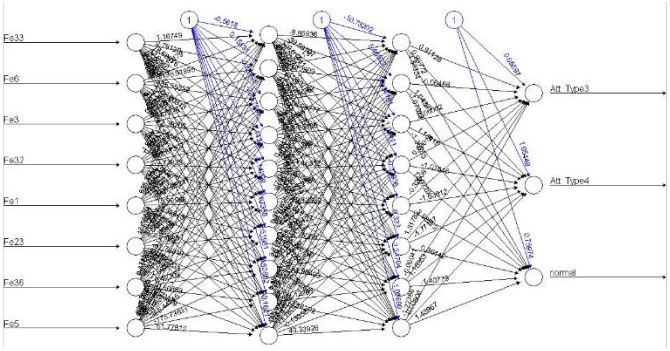

Figure 9: ANN network with ten neuron at layer 1 and eight neurons at layer 2

Table 6: Accuracy of ANN model with different neurons at different layers.

Minor Dataset				
ANN Model				
S. No.	Layer 1(neurons)	Layer 2(neurons)	Layer 3(neurons)	Accuracy (%)
1	4	0	0	96.77
2	4	2	0	97.78
3	4	4	0	97.91
4	6	2	0	98.77
5	6	3	0	97.28
6	6	4	0	98.51
7	6	6	0	98.49
8	10	8	0	99.47
9	6	2	4	98.25

The observed results shows that the Random Forest model has given best accuracy with 99.886 % for Att_Type_3 attacks, 99.795% for Att_Type_4 attacks and accuracy of 99.21% for normal data traffic.

In Level I of the proposed approach the model is trained with Artificial Neural Network (ANN). The different numbers of neurons in the hidden layer is taken and the results are observed. The selected 8 features are minor dataset is used to train the model. ANN model with 4 neuron in hidden layer has an accuracy of 96.77 %, model with 4 neuron in hidden layer 1 & 2 neurons in layer 2 has an accuracy of 97.91 %, model with 4 neurons in hidden layer 1 & 4 neurons in hidden layer 2 has an accuracy of 97.91 % , model with 6 neurons in hidden layer1 & 2 neurons in hidden layer 2 has an accuracy of 98.77 %, model with 6 neurons in hidden layer 1 & 3 neurons in layer 2 has an accuracy of 97.28% and model with 6 neurons in hidden layer 1 & four neurons in hidden layer 2 has an accuracy of 98.51%.

The experimental results (Table 6) shows that, a ANN model with six neurons at layer 1 & six neurons at layer2 has an accuracy of 98.49 % and with ten neurons at layer 1 & 8 neurons at layer2 has an accuracy of 99.47%. When the layer of the ANN model is increased to three the accuracy of the model decreased. A model with six neurons at layer 1 , two neurons at layer 2 & four neurons at layer 3 has accuracy of 98.25% which less than two layered ANN model.

6. CONCLUSION AND FUTURE WORK

The results showed that, Level I in proposed approach gives best accuracy by using an ANN algorithm having ten neurons at layer 1 & eight neuron at layer 2. The accuracy of Level I is 99.46%. Precision for Att_Type3 is 97%, Att_Type4 is 98% and for normal traffic is 99%. Recall rate of 87% for Att_Type3, 96% for Att_Type_4 and 99% of normal traffic is achieved (Table 7).

Table 7: ANN model accuracy, precision and recall rate

ANN model for Rare attacks(Layer1:10 and Layer2:8 neurons)			
	Att_Type3	Att_Type4	normal
precision	0.97	0.98	0.99
recall	0.87	0.96	0.99
accuracy	0.99465		

The comparison of results with the existing models shows that the proposed approach outperform for the minor or rare attacks. The accuracy of 99.46 % is much better than previously proposed models Table 8.

Table 8: Comparison of the proposed approach with exist models

Accuracy of the Models proposed (%)		
Reference Number	Att_Type_3	Att_Type_4
[16]	73.2	99.9
[6]	90.72	89.28
[17]	48.2	87.3
[18]	96.4	65.4
In Proposed Approach	99.46	

The level I is further training by increasing the number of records in training dataset by using SMOTE[19] algorithm. The re training model was able to identify novel attacks of the NSL KDD test dataset. Overall Level II for major attack an accuracy above 99.5 is achieved and at level I accuracy of 99.46 is achieved.

Further the proposed approach accuracy can test for different dataset set. Other machining learning approach can be considered to further improve the accuracy of overall system.

REFERENCES

1. N. Sheikh, K. Mustafi, and I. Mukhopadhyay, "**A Unique Approach to Design an Intrusion Detection System using an Innovative String Searching Algorithm and DNA Sequence**," 2016.
2. M. Tabatabaefar, M. Miriestahbanati, and J. C. Gregoire, "**Network intrusion detection through artificial immune system**," in *11th Annual IEEE International Systems Conference*, SysCon 2017 - Proceedings, 2017.
3. T. Zou, Y. Cui, M. Huang, and C. Zhang, "**Improving performance of intrusion detection system by applying a new machine learning strategy,**" *Proc. 5th Int. Conf. Soft Comput. as Transdiscipl. Sci. Technol. - CSTST '08*, p. 51, 2008.
4. U. R. Salunkhe and S. N. Mali, "**Security Enrichment in Intrusion Detection System Using Classifier Ensemble**," *J. Electr. Comput. Eng.*, vol. 2017, 2017.
5. M. S. Mohd Pozi, M. N. Sulaiman, N. Mustapha, and T. Perumal, "**Improving Anomalous Rare Attack Detection Rate for Intrusion Detection System Using Support Vector Machine and Genetic Programming**," *Neural Process. Lett.*, vol. 44, no. 2, pp. 279–290, 2016.
6. N. Sharma and S. Mukherjee, "**Layered approach for intrusion detection using naïve Bayes classifier**," *Proc. Int. Conf. Adv. Comput. Commun. Informatics - ICACCI '*12, p. 639, 2012.
7. S. Dhivya, D. Dhakchianandan, A. Gowtham, P. K. Sujatha, and A. Kannan, "**Memory efficacious pattern matching intrusion detection system**," *2013 Int. Conf. Recent Trends Inf. Technol. ICRTIT 2013*, pp. 652–656, 2013.
8. A. A. Aburomman and M. B. I. Reaz, "**Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection,**" in *Proceedings of 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2016*, 2017, pp. 636–640.
9. A. Hadri, K. Chougdali, and R. Touahni, "**Intrusion detection system using PCA and Fuzzy PCA techniques**," in *2016 International Conference on Advanced Communication Systems and Information Security, ACOSIS 2016* - Proceedings, 2017.
10. R. Bala, "**A review on kdd cup99 and nsl-kdd nsl kdd dataset**," *www.ijarcs.info* vol. 10, no. 2, 2019.
11. T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "**BAT : Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset**," vol. 8, pp. 29575–29585, 2020.
12. S. Gurung, "**Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset**," no. March, pp. 8–14, 2019.
13. S. Choudhary and N. Kesswani, "**ScienceDirect Analysis Analysis of and UNSW-NB15 UNSW-NB15 Datasets Datasets using Deep Learning in IoT using Deep Learning in IoT**," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 1561–1573, 2020.
14. "**NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB**." [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html. [Accessed: 17-May-2020].
15. O. Decision, "**6. Learning Vector Quantization**," 1995.
16. P. G. Jeya, M. Ravichandran, and C. S. Ravichandran, "**Efficient Classifier for R2L and U2R Attacks**," *Int. J. Comput. Appl.*, vol. 45, no. 21, p. 29, 2012.
17. K. C. Khor, C. Y. Ting, and S. Phon-Amnuaisuk, "**A cascaded classifier approach for improving detection rates on rare attack categories in network intrusion detection**," *Appl. Intell.*, vol. 36, no. 2, pp. 320–329, 2012.
18. C. Science and K. Mangalore, "**A Two-tier Network based Intrusion Detection System Architecture using Machine Learning Approach**," pp. 42–47, 2016.
19. N. V Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "**SMOTE : Synthetic Minority Over-sampling Technique**," vol. 16, pp. 321–357, 2002.