Implementation of Machine Learning Techniques applied to the Network Intrusion Detection System

B Ida Seraphim, Shreya Palit, Kaustubh Srivastava, E Poovammal

Abstract: An immense amount of data is being generated every second due to technological advancement and reforms. Social networking and cloud computing are generating a huge amount of data every second. Every minute data is being captured in the computing world from the click of the mouse to video people tend to watch generating an immediate recommendation. Everything a user is doing on the internet is being captured in different ways for multiple intents. Now it all ends up to monitor the system and network and, secure lines and servers. This mechanism is called Intrusion Detection System(IDS). Hacker uses multiple numbers of ways to attack the system which can be detected through a number of algorithm and techniques. A comprehensive survey of some major techniques of machine learning implemented on intrusion Detection was done where techniques based on k-means, K-means with principal component analysis, Random Forest algorithm Extreme learning the ma-chine, techniques, classification algorithms such as Naive Bayes algorithm, Hoeffding Tree algorithm.Also, Accuracy Updated Ensemble algorithm, Accuracy Weighted Ensemble algorithm, Support Vector Machine, Genetic algorithm and Deep learning were studied. Now some of these algorithms are applied upon the NSL-KDD data set and compared on the basis of their accuracy.

Index Terms: IDS, Artificial Neural Networks, One Hot Encoding, Probe Attack, Feature Selection

I. INTRODUCTION

The IDS can be distinguished on the basis of where the detection is taking place and how or by which technique it is being detected. The IDS is classified into two niche segment one being Network Intrusion Detection System(NIDS) and the other being Host Intrusion Detection System(HIDS). the first system mentioned helps in the analysis the incoming networking traffic whereas the HIDS functioning is based on the activity of the operating system. The IDS that is based on the method of detection being applied which can be classified as the Signature based (misuse) detection, which acknowledges inadequate model - anomaly detection method and analyzes the deviations of the network from a “good” model using Machine Learning techniques.

There are essentially two main challenges that arise while generating an effective IDS for new attacks. First, the feature selection from the dataset is very difficult as it will tell us how important a feature can be. The feature selection changes with the change in attack type. Secondly, there does not exist a labeled traffic real-time networking. [1] Data Mining is an analysis technique that is used to analyze Big Data. Data Mining techniques were first applied to the IDS in 1998. The main aspects of data mining on IDS that were dealt with originally were termed as clustering and classification. Since there exist no label for the initial data set for clustering issue, the object created for the clustering algorithm was allocated the same class with similar data records. The behavior of the packet was termed as a normal class or abnormal class according to the features and characteristics of already existing data. In Classification, which works on mining from the already clustered data. This implies that the data is labeled. As time has passed by, numerous techniques have been used for data mining but the recent researches are using the concept of Deep Learning and Neural Networks to implement an effective IDS. [2] Clustering is the process of creating the partition on data such that each partition or group has the same characteristic. A similar pattern is found out between the data and then on the basis of it, the data is segregated. Clustering has a significant benefit in the intrusion detection system that it can learn from the record or the audit data itself. Mini-batch K-means clustering is also an upcoming concept in the data mining field where the concept of K- means is used over IDS. Minibatch K-means algorithm’s principal idea is using different random groups of distinct memory size so that they can be easy to store. Each group of data is computed under the algorithm and the output is again fed into the process. [3] Classification is a data mining technique which is used for examining a data set. In this world of continuous streaming data, classification plays an important role in classifying the data. Many algorithms such as decision tree, rule-based in-duction, neural network, Bayesian network, genetic algorithm etc are used to classify the data. Now ensemble model is being used under a classification which helps to give a low false alarm and high accuracy. Classifier Ensemble Accu-racy(AUE) is an updated version of the accuracy weighted ensemble(AWE) data mining algorithm. It uses the concept of updating a classifier according to the distribution. [4] Genetic Algorithm is used to improve the efficiency which is based on the principles of Genetics and certain environmental factors.

Manuscript published on 30 June 2019.
* Correspondence Author (s)

B.Ida Seraphim, Department of Computer Science and Engineering, SRM IST, Kattankulathur, Tamil Nadu, India
Shreya Palit, Department of Computer Science and Engineering, SRM IST, Kattankulathur, Tamil Nadu, India
Kaustubh Srivastava, Department of Computer Science and Engineering, SRM IST, Kattankulathur, Tamil Nadu, India
E Poovammal, Department of Computer Science and Engineering, SRM IST, Kattankulathur, Tamil Nadu, India

In the training process of the genetic algorithm, a fixed rule is formed from the analyzed data using Genetic Algorithm and then the data is tabulated in forms of a large number of rules which could be used in the monitoring of IDS

Deep learning is a type of classification process which can be used to classify the attack type and raise an alarm. Deep learning autoencoder is one the deep learning algorithm which can be used to monitor IDS. Autoencoder basically has three layers, first is the input layer, second, is the so called hidden layer and third being same as the first layer called the output layer. The input layer and the output layer has the same number of attributes or parameters. It basically creates a function so as to bring the output same. Network Intrusion Detection System is the most extensively used security technology in the field of network security. In recent years many techniques and algorithms have been built to improve the monitoring of network intrusion detection system.In this paper, a comprehensive survey of some major techniques of machine learning implemented on intrusion De-tection is presented. Techniques based on k-means, K-means with principal component analysis, Random Forest algorithm Extreme learning the machine, techniques, classification al-gorithms such as Naive Bayes algorithm, Hoeffding Tree algorithm.Also Accuracy Updated Ensemble algorithm, Accu-racy Weighted Ensemble algorithm ,Support Vector Machine, Genetic algorithm, and Deep learning to use Autoencoders etc have been implemented. We want to implement the intrusion detection system us-ing Deep Learning which uses a two-level approach. In the first level of implementation, we will implement a super-vised/unsupervised learning algorithm. In Level 2 approach we would train the results from level 1 in deep learning using Deep learning and compare the major 5 parameters Accuracy, Precision, Recall, False Alarm, F-score. [5]

I. DATASET

Technology is rapidly changing day by day, and hence a lot of inventions and technology advancements are being done in order to protect Computer Systems from any network intrusions attacks. Research on the network intrusion attacks, usually used the available KDD Cup 1999 data set. This data set was used on various machine learning algorithms. But this dataset was seen of having many problems. Firstly, one of the main disadvantages of the KDD data set is the number of redundant records in the dataset. In the training set 78% of records are duplicated while in the testing dataset around 75% of the total number of records are duplicated , and hence shifting our results on the learning algorithms to come out as biased. Though, available as a public data set for the network intrusion detection system is very limited,a new version of KDD Cup 99 data set is available which is known as the NSL KDD dataset Now researches are using the dataset to apply at the machine learning algorithms to it. The new NSL KDD test and train dataset combines only very selected data records from the original KDD dataset and the redundancy of records do not exist. Hence, it being declared as a standard dataset and the research evaluation results be consistent over all researches. The training dataset is made up of basically four types of attack Classes. They are ,first the Denial of Service(DoS), second is called Probe Attack, Third is termed as User to Root(U2R) and the last one is Root to Local(R2L). This in turn are made up of more than 21 different attacks. [6]

I. LITERATURE REVIEW

A. CLUSTERING

Mini batch K-means clustering is the trending clustering algorithm used for intrusion detection system. Here it basically focuses on the application of K-means on the IDS. Mini bath K-means algorithm's main idea is the usage of different, purely random groups of particular memory size so that they are easy to store. Each computation on the random sample of the group of the dataset is extracted and updated in the cluster. This process is repeated until a converged. These ran-dom groups are termed as mini-batches. The Documentation initially proposes an interconnected algorithm on K-means clustering and C4.5 algorithm for detection of the anomaly. At the end , an improved IDS K-Means algorithm was proposed. Mini Batch K-means clustering algorithm and IDS clustering method names PMBKM with the use of Principal Component Analysis(PCA) was proposed. First, the preprocessing of the data was done by converting the strings into digital for and then normalizing the data for enhancing the effectiveness of clustering. Secondly, PCA was used to diminish the dimension of the data by applying feature selection.

TABLE I
NUMBER OF VALUES DIVIDED AMONG THE TRAINING DATA SET

Attack type	Records
Normal	67,343
Denial of Service(DoS)	45,927
Probe	11,656
User to Root	52
Root to Local	995

TABLE II
NUMBER OF VALUES IN THE TESTING DATA SET

Attack type	Records
Normal	9711
DoS	7456
Probe	2421
U2R	200
R2L	2756

Finally, Mini Batch K-means was used into the field of the big data. K means++ was used to improve the clustering efficiency and to avoid any local optimum created during the implementation.

B. CLASSIFICATION

Classification is a data mining technique which is used for analyzing a data set. In this fast changing world of continuous generation of streaming data, classification plays an important role in classifying the data. In a conference presented by Ketan Sanjay Desale, Chandrakant Namdev Kumathekar , Arjun Pramod Chavan they write about the following clas-sification algorithms being applied in IDS. Many algorithms such as Naive Bayes algorithm, Hoeffding Tree algorithm. Also, Accuracy Updated Ensemble algorithm and Accuracy Weighted Ensemble algorithm are the types mentioned by them. The Naive Bayes algorithm is a probability based method. Naive Bayes classification is a very useful method to solve detection and prognosis nature of problems. The above mentioned algorithm uses conditional probability to create a Naive Bayes classier on the basis of which classification is done. In IDS, Bayes Classifier is used to find the Accuracy, Statistic Kappa and time decision based parameters.

Classifier Ensemble Accuracy(AUE) is an updated version of the accuracy weighted ensemble(AWE) data mining algorithm. It uses the concept of updating a classifier according to the distribution. Ensemble Weighted Classifier is represented as a cost function which defines the following (1) a date numerical value with the aim to decrease or minimize the misclassification rate (2) a numerical term with aim to decrease number of classifiers and (3) a non-negative constraint on the weights of the classifier. [7] [8]

C. DEEP LEARNING

In computational intelligence, a work done by Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai , and Qi Shi proposed non symmetric deep auto encoder (NDAE) for unsuper-vised learning and with the use of classification model such as deep learning which was programmed employing NDAEs for intrusion detection system. They have evaluated their proposed model using the upgraded KDD Cup’99 ,the NSL-KDD data sets to overcome the challenges of Volume, Accuracy, Di-versity, Dynamics, Low-frequency attacks, Adaptability. Deep Learning is an artificial intelligence function that tries to work equivalent to the human brain in processing data and deduce patterns. They used Autoencoder to learn a present for a set of data for dimensional reduction and finally assessed their outcome on the 5 parameters, namely, Accuracy, Precision, Recall, F-score, and lastly the False Alarm. The proposed model claimed to have accomplished an accuracy of 97.85% which was the best possible accuracy model in the present interval. [9]

IV. ATTACK CLASSES

As mentioned above there are 4 types of attack classes-DoS(Denial of service),R2L(Root to Local),U2R(User to Root) and Probe Attack.Short Descriptions for the same are given below:

DoS : It is a class of attack where the attacker restricts processing time of the resources so as to avoid the genuine user from obtaining those resources.The main objective of Denial of service(DoS) attack type restrain or prevent the legitimate user from accessing the services and resource of the services. This type of attack aims the availability of network which causes the excessive usage of the network, consuming the main resources of the system. This type of attack occurs when the legit user is not able to use the resources and the attacker is using most of the network to gather the resources it needs. There are many techniques for an intrusion detection system for classifying the attack type. Each packet has been divided into 41 parameters and the combination of some parameter will determine whether any anomaly is happening or not. R2L: attacks are illegal access from a remote system.R2L attack are both categorized under network based and host-based network intrusion detection system and thus both the features are taken up. In this, the attacker sends up a message to the server and make some changes to the server in order to get resources. U2R: In this, the attack the attacker tries to gain the password of the user and then get into the system as a legitimate user and retrieve the data.in this case, it main even try to get the server control in order to have full access.

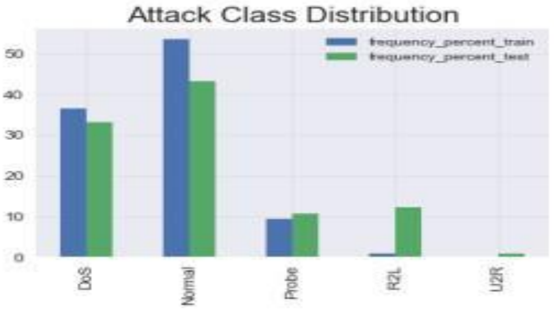


Fig. 1. The percentage division of attack classes in the training and testing dataset

Probe attack: The Attacker will examine the network to collect information and would make some breach in the future. In addition to this we also have a class describing the Normal class, which do not depict any kind of attacks on the network intrusion detection system. Here they depict the normal condition of the intrusion detection system.

V. IMPLEMENTATION

The implementation of the Network intrusion detection After this implementation we implement our own model based on Artificial Neural Network and then compare the results between ANN,Decision tree,Simple Logistic Regresion and KNN Neighbor Classifier.

A. MODULES DESCRIPTION

1) SciKit Learn: Scikit -learn was developed by David Cournapeau in his google summer of code project in the year of 2007.Scikit-learn gives a series of supervised and unsupervised learning algorithms by an interface in Python. It is commissioned under a simplified BSD license and is filed under many Linux configurations. The library is formed under the Scientific Python that must be fixed before you can use scikit-learn. This Scikit includes NumPy, SciPy, Pandas etc. This package is used intrusion detection system to bring up the package NumPy and Pandas for data analysis of the NSL KDD dataset.

2) Keras: Keras is a basic Python library which is used for deep learning that can run with tensor-flow. It was made to make implementing deep learning models as swift and easy as possible for research. It runs on Python and can very easily be executed on GPUs and CPUs.Keras was extended and sustained by François Chollet using some guiding principles:

Modularity: A model can be interpreted as a series or a graph. All the concerns of a deep learning model are discrete elements.

Minimalism: The library gives enough to achieve an outcome. Extensibility: New elements are quite easy to add and use within the framework and is intended for researchers to explore new ideas.

B. SIMPLE LOGISTIC REGRESSION and K NEIGHBOUR CLASSIFIER

1) Data Pre-processing:: The NSL KDD dataset is made up of 41 features. Since taking all the 41 features in consideration is not possible we plotted a feature importance graph. The feature importance graph gave us a clear picture of the All features and its variation in the values. By this we took the decision of dropping the last 9 as there are no variations in the value attached to those. Some of the columns like su_attempted,srv_rerror_rate,urgent,is_host_login, num_shells, land have only 0 as their value. Hence, we decided to drop them in out preprocessing of the dataset. [10]

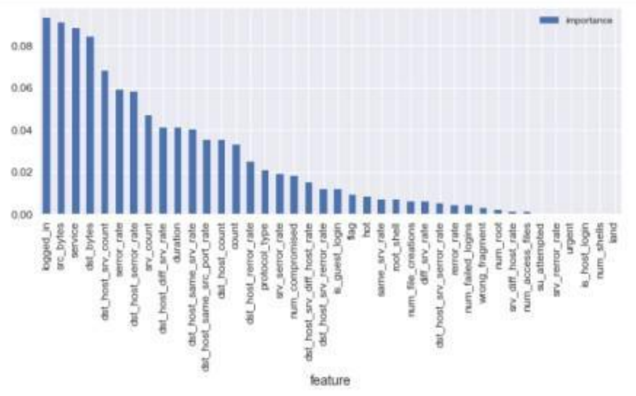


Fig. 2. Feature Importance graph

After this we extract the numerical attributes and scale it to have zero mean and unit variance by changing it from the float16 and Int16 format, and then adding That into a new numpy data frame.

Another major part of preprocessing of the dataset includes the way, we are dealing with the categorical attributes. Firstly, we extract the categorical attributes from both training and testing data sets. Once done, we encode the categorical at-tributes using the LabelEncoder from the Scikit Learn package.

One Hot Encoder is a mechanism by which categorical variable goes under transformation accepting the value 1 if true and 0 if false. This type of encoding is very easy to use but it can be voluminous to try to implement it using scikit-learn in Python, as there isn't currently a simple transformation method for it.

The pre-processing operation has to be performed because the dataset Contains both the types, numerical as well as the non-numerical data records. The scikit works perfect with numeric values and thus we try to convert the categorical records to Binary form. The technique will convert each categorical feature with m possible inputs in comparison to the n binary feature.

The features are scaled to avoid features with large values that may weigh too much in the results. [11] 4

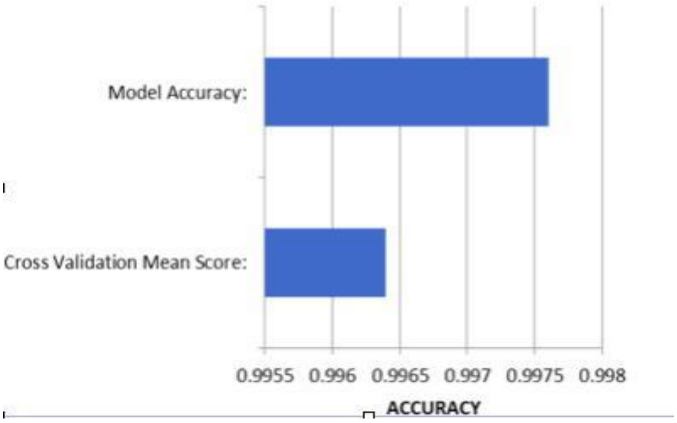


Fig. 3. KNeighbour Classifier Model

2) Feature Selection:: Elimination of any redundant data is done by selecting from subset of relevant features, by representing the full problem. Once done, we fit the data frame of testing and training dataset.

We create two target classes, one is called the normal class and the other is called the attack class. A function is created which subdivides the train and test dataset into two-class attack labels [12]

3) Build the model:: We build two models on the basis of two classifiers, a KNeighbour Classifier and a logistic regression classifier. Both of the above mentioned models are present in the scikit-learn module.

4) Prediction & Evaluation (validation): : Using the test data to make predictions of the model. Multiple scores are considered such as accuracy score, then recall, the f-measure, an confusion matrix. Perform a 10-fold cross-validation.

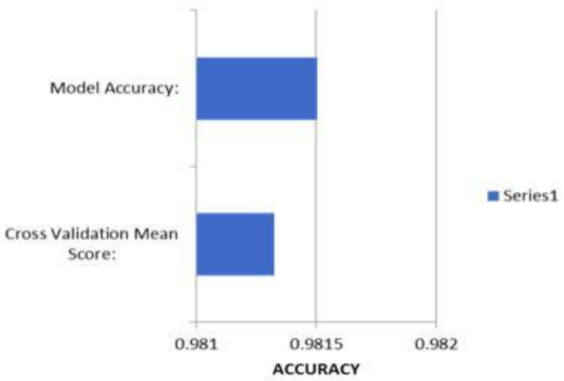


Fig. 4. Logistic Regression Classifier

C. DECISION TREE

The subset feature eliminating Mechanism for Intrusion Detection System directly based on the Decision Tree. This work is done to rightly implement the work done by Herve Nkiama , Syed Zainudeen Mohd Said , Muhammad Saidu .

1) Step 1: Data Cleaning andt the Pre-Processing: The first step in the dataset is it has to undergo by a cleaning process to eliminate duplicate records. Next a Pre-processing step will have to be done and taken in place because the dataset contains both the numerical and the non-numerical instances. Generally the so called estimator (classifier) defines in the scikit-learn adapts well with number inputs, so a one-of-K or the famous - one-hot encoding method is used to make that transformation. This technique will help to transform each categorical value with m possible inputs to n binary features.

2) Step 2: Feature Selection: Feature Selection also known as variable selection or subset extraction plays an important part here. After preprocessing of data takes place, Elimination of redundant and irrelevant data by selecting a subset of rele-vant features. This is done using a Univariate feature selection with ANOVA F-test. This test is used to do a thorough analysis for each of the feature one by one to determine the full strength of the relationship between the feature and labels. They used a SecondPercentile method (sklearn.feature_selection) to select features depending upon percentile of the highest scores. When the particular subset is found: Recursive Feature Elimination (RFE) was applied.

3) Step 3: Build the model: Decision tree model is built using the steps above.

4) Step 4: Prediction & Evaluation (validation): Using the test data to make predictions of the model, here they found the Accuracy score, recall, f-measure separately for each attack class to the normal class. For a comparison with other models we use the average of all these modules.

D. ARTIFICIAL NEURAL NETWORKS

Artificial neural networks are one of the main upcoming and tools being used in machine learning. Neural as the name suggests is related to the brain network systems, they are intended to replicate the way humans learn things.

The architecture of Neural network comprises layers Neural networks consist of input and output layers, as well as a hidden layer. This hidden layer consists of values that convert the input values into something that the output layer can use. The models are trained in epoch cycles, and every time by fine-tuning the parameters to improve the accuracy. [13]

1) Methodology: We know already that the Train+/Test+ data sets include sample difficulty rating and the attack classes.

The traffic can be grouped into 5 categories: Normal, DOS, U2R, R2L, Probe or more coarsely into Normal vs Anomalous that is any variation seen from the for the binary classification task. An attack map is created in a sorted order according to the class labels. We apply a fairly simple ANN architecture . We use the concept of auto encoders.

An auto encoder is a type of artificial neural network used to learn efficient data codings in an unsupervised man-ner.Autoencoders main aim is to learn the encoding if data , they learn it using dimensional reduction. They inturn try to reduce any noise from the ANN model. Reduction in autoencoder is not alone, we often see it is accompanied by restructuring or reconstructing of whatever it has learn, it tries to restructure it as closes it can be to the output. Recently, the autoencoder concept has become more widely used for learning generative models of data. They are excellent tools for finding patterns which are far too complex or numerous for a human programmer to extract and teach the machine to recognize.

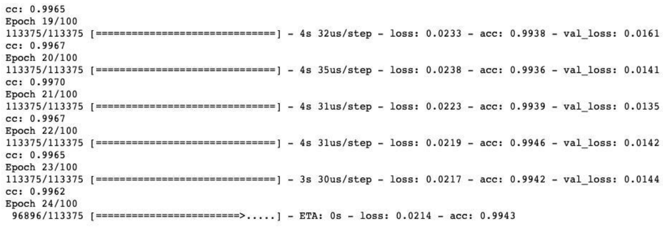
While building the network we take care that we add the features in a sequential way and we add the activation function as ReLu.In the context of artificial neural networks, the rectifier is an activation function defined as the positive part of its argument:

f (x) = x+ = ma x(0; x)

x is the input of neuron

This is also known as ramp rectification in the field of electrical engineering.

After building the network and fine-tuning parameters , we see in an epoch of 100 with a validation split = 0.1, we get an accuracy after training the model to be shown as 0.9943 [14]



```
cc: 0.9965
Epoch 19/100
113375/113375 [==============================] - 4s 32us/step - loss: 0.0233 - acc: 0.9938 - val_loss: 0.0161
cc: 0.9967
Epoch 20/100
113375/113375 [==============================] - 4s 35us/step - loss: 0.0238 - acc: 0.9936 - val_loss: 0.0141
cc: 0.9970
Epoch 21/100
113375/113375 [==============================] - 4s 31us/step - loss: 0.0223 - acc: 0.9939 - val_loss: 0.0135
cc: 0.9967
Epoch 22/100
113375/113375 [==============================] - 4s 31us/step - loss: 0.0219 - acc: 0.9946 - val_loss: 0.0142
cc: 0.9965
Epoch 23/100
113375/113375 [==============================] - 3s 30us/step - loss: 0.0217 - acc: 0.9942 - val_loss: 0.0144
cc: 0.9962
Epoch 24/100
 96896/113375 [========================>.....] - ETA: 0s - loss: 0.0214 - acc: 0.9943
```

Fig. 5. Accuracy after the 24 Epoch cycle

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

VI. EXPERIMENTAL RESULTS AND DISCUSSION

A comparison study between the Logistic Regression Clas-sifier , KNeighbour Classifier , Decision tree model and the model based on Artificial Neural Network is given below:

TABLE III
EXPERIMENTAL RESULTS A COMPARISON

TYPE OF MODEL	ACCU-RACY	PRECISION	RE-CALL	F SCORE
LOGISTIC REGRESSION	0.85	0.85	0.85	0.85
KNEIGHBOUR CLASSIFIER	0.87	0.88	0.87	0.87
DECISION TREE	0.97	0.86	0.91	0.88
ARTIFICIAL NEURAL NETWORK	0.9946	varies with tuning parameters	-	-

For a better representation to the above results we can use the way of confusion matrix, we can aggregate the model pre-dictions and then represent them. This will help to understand the differences and refine the model for subsequent usage. The Artificial Neural Network model does not give conclusive results on the U2R and R2L, due to parameter variations in every epoch cycle.

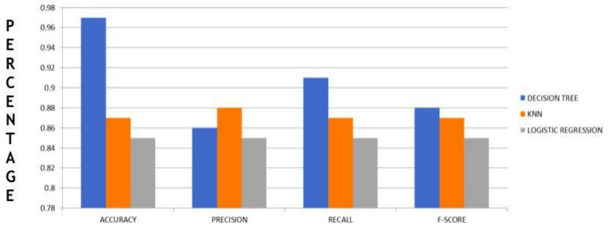


Fig. 6. GRAPHICAL COMPARISON TO MODELS

The above values are combination of the related works and implementing the models, there are many possibilities to restructure the models and get another set of results for comparison.

VII. CONCLUSION

Network Intrusion Detection System is the most used defense technology in the domain of network security. In recent years many of the techniques have been implemented for the intrusion detection system.

In this paper, a detailed survey of major techniques implemented on intrusion Detection is presented. Techniques based on k-means, K-means with principal component analy-sis, Random Forest algorithm Extreme learning the machine, techniques, classification algorithms such as Naive Bayes algorithm, Hoeffding Tree algorithm, Accuracy Updated En-semble algorithm. Also, Accuracy Weighted Ensemble algo-rithm ,Support Vector Machine, Genetic algorithm and Deep learning to use Autoencoders etc have been implemented.

We do a comparison of experimental values a system where we try to increase the efficiency of the parameters in the intru-sion detection system using the two-level approach. In Level 1, We would like to compare any basic supervised/unsupervised learning algorithm and then in Level 2 we would train the results from level 1 in deep learning to use Artificial Neural Networks(ANN) and compare the parameters such Accuracy, Precision, Recall, False Alarm, F-score. We expect that the im-plementation of artificial neural networks. Though we compare all the attack classes, in the Artificial Neural Network model we were not able to take in consideration the U2R and R2L attack classes. A future model incorporating our drawback can be modeled.

REFERENCES

1. “Types of Intrusion Detection System.” [Online]. Available: https://en. wikipedia.org/wiki/Intrusion_detection_system
2. K. S. Desale, C. N. Kumathekar, and A. P. Chavan, “Efficient Intrusion Detection System using Stream Data Mining Classification Technique,,” in International Conference on Computing Communication Control and Automation,, 2015.
3. K. A. I. PENG, V. C. M. LEUNG, and Q. HUANG, “Clustering Approach Based on Mini Batch Kmeans for Intrusion Detection System Over Big Data,” SPECIAL SECTION ON CYBER-PHYSICAL- SOCIAL COMPUTING AND NETWORKING, , 2018. [Online]. Available: 0.1109/ACCESS.2018.2810267
4. AHMAD, M. BASHERI, M. J. IQBAL, and A. RAHIM, “Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection.” [Online]. Available: 0.1109/ACCESS.2018.2841987
5. Q. Niyaz, M. Alam, W. Sun, and A. Y. Javaid, “A Deep Learning Approach for Network Intrusion Detection System,,” in Conference Paper in Security and Safety, 2015.
6. S. Revathi and D. A. Malathi, “A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion De-tection,” International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 12, 2013.
7. “Mrutyunjaya Panda and Manas Ranjan Patra, “Network Intrusion Detection using Naive Bayes”,” International Journal of Computer.
8. “Sparsity-driven weighted ensemble classifier.” [Online]. Available: https://arxiv.org/abs/1610.00270
9. Z.WANG, “DeepLearning-BasedIntrusionDetectionWithAdversaries,”
10. SPECIAL SECTION ON CHALLENGES AND OPPORTUNITIES OF BIG DATA AGAINST CYBER CRIME, 2018. [Online]. Available: 10.1109/ACCESS.2018.2854599
11. H. su Chae and S. H. Choi, “Feature Selection for efficient Intrusion Detection using Attribute Ratio,” INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS , vol. Volume 8, 2014.
12. Prof.S.S.Manivannan and Dr.E.Sathiyamoorthy, “An Efficient and Ac-curate Intrusion Detection System to detect the Network Attack Groups using the Layer wise Individual Feature Set ,” International Journal of Engineering and Technology (IJET).
13. H. Nkiama, S. Z. M. Said, and M. Saidu, “A Subset Feature Elimination Mechanism for Intrusion Detection System,” (IJACSA) International Journal of Advanced Computer Science and Applications,, vol. Vol. 7, no. No. 4, 2016.
14. “Artificial Neural Networks Defination.” [Online]. Available: https: //www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/
15. R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Applying con-volutional neural network for network intrusion detection.” in ICACCI 2017, pp. 1222–1228.