Intrusion Detection techniques for detection of Cyber Attacks

Shaikh Sahil Ahmed[1], Mahesh Kankar[1], and Bhawana Rudra[1]

National Institute of Technology Karnataka
sahilahmed786001@gmail.com mahesh15kankar@gmail.com
bhawanarudra@nitk.edu.in

Abstract. Intrusion Detection System (IDS) is a software-related application where we can detect the system or network activities and notice if any suspicious task happens. Excellent broadening and the use of the internet lift examines the communication and save the digital information securely. Now a days, attackers use variety of attacks for fetching private data. Most of the IDS techniques, algorithms, and methods assist to find those various attacks. The central aim of the project is to come up with an overall study about the intrusion detection mechanism, various types of attacks, various tools and techniques, and challenges. We used various machine learning algorithms and found performance metrics like accuracy, recall, F-measure, etc and compared with the existing work. After this research, we got good results that can help to detect the cyber attacks being performed in the network.

Keywords: Intrusion Detection · Cybersecurity · Machine Learning · Computer Networks.

1 Introduction

Intrusion Detection Systems (IDSs) are a range of cybersecurity based technology at first developed to find the exploits and vulnerabilities against a destination host. The individual use of the IDS is to detect threats. Algorithms of machine learning have played an necessary part in the field of cybersecurity. The fundamental way is to use machine learning algorithms to build a model of honest and reliable activity, and then it is compared to the new behavior against this model [7,8,9,10,11,12].
We evaluated our project based on various performance metrics such as accuracy, recall, precision, f-measure, and entropy. Accuracy is defined as the ratio of the number of correct assumptions to the total number of input samples, precision (also called positive predictive value) is defined as the fraction of necessary samples among the retrieved samples, while recall (also known sensitivity of data) is the part of the total number of necessary samples that were actually retrieved. The F-measure (F1 score) is a computation of a test's precision and it is defined with the weighted harmonic mean of the accuracy and recall of the test. Entropy is a measure of the randomness in the information being processed.

2 Literaure Review

Ansam Khraisat [2] discussed various techniques of Intrusion Detection System such as statistics-based techniques, Knowledge-based techniques, Supervised learning, Unsupervised learning, Semi-supervised learning, Hybrid based techniques, etc. Attacks are classified into four categories into Denial-of-Service (DoS), Probing, User-to-Root (U2R), and Remote-to-Local (R2L). They have compared various datasets such as NSL-KDD, ADFA-WD, ADFA-LD, etc. In their paper, they have presented, in detail, a survey of intrusion detection system methodologies, types, and technologies with their advantages and limitations.
Mr. Mohit Tiwari [3] discussed various techniques such as an Anomaly-based detection system and signature-based intrusion detection. They also discussed two types of IDS as client-based and network-based. Two models described are local (one system to monitor) and client/server for centralized analysis.
Rachna Kulhare [5] discussed the detection and prevention of cyber-attacks and also about various types of IDS. They surveyed different approaches such as pattern matching, fuzzy clustering, etc. They concluded that the study of IDS is great for network security.
Bane Raman Raghunath [6] discussed the supervised anomaly detection that shows how anomalous the network is an association pattern analysis indicating the network as highly anomalous. Further, they are given a very huge amount of connections observed per given unit time which is more useful for the detection of attacks.
Yuyang Zhou [12] discussed propose a heuristic algorithm called Correlation-based Feature-Selection Bat Algorithm (CFS-BA) to detect the cyber attacks. They performed experiments using KDDCup 99, NSL-KDD, and CIC-IDS2017 datasets. They got good accuracy and examined various performance metrics. They proposed a novel machine learning-based IDS. Firstly, they propose a CFS-BA algorithm with the aim of discarding irrelevant features. Then, the ensemble classifier based on C4.5, Random Forest and Forest by Penalizing Attributes with the average of probabilities rule is used to construct the classification model. The proposed IDS is evaluated on KDDCup'99, NSL-KDD and CIC-IDS2017 datasets.

3 Methodology

Till now, we worked on KDD Cup 99 dataset. This dataset is grouped together by almost 49,00,000 individual connections which include a feature count of 41. The simulated attacks were categorized as given below :

1. **Denial-of-Service-Attack (DoS) :** Host becomes inaccessible due to flooding and hence the host is overloaded.
2. **User-to-Root-Attack (U2R) :** unauthorized access from a remote machine.
3. **Remote-to-Local-Attack (R2L) :** unauthorized access to local superuser (root) privileges.

4. Probing-Attack : surveillance and other probing.

The dataset contains 42 features like duration, protocol_type, service, src_bytes, dst_bytes, etc. Various attacks are labeled under the label attribute present in the 42nd index of the dataset. Based on the dataset of attacks collected in the past, we build and train our model so that the machine can detect future attacks (suspicious activity) going in the network. The dataset contains the attacks under each of 4 cases as shown in table 1.

Table 1. Category and types of attack.

Category of Attacks	**Types of Attacks**
Denial-of-Service-Attack (DoS)	back, land, neptune, pod, smurf, teardrop.
User-to-Root-Attack (U2R)	Buffer_overflow, loadmodule, perl, rootkit.
Remote-to-Local-Attack (R2L)	Ftp write, guess passwd, multihop, spy, imap, phf, warezclient, warezmaster.
Probing-Attack	Ipsweep, nmap, portsweep, satan.

Various Machine Learning algorithms used are Deep Neural Network (with one and five layer), Artificial Neural Network (ANN), Naive Bayes, Logistic Regression, Decision Tree and Random Forest.

4 Implementation

All the experiments are performed over the dataset "kddcup.data_10_percent.gz" as mentioned in [1]. The dataset contains 494020 rows. We used 70% of the dataset for training purposes and the remaining 30% for testing purposes. We go through various algorithms and get the performance metrics of the work done as shown in Table 2.

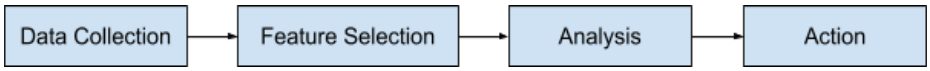

Fig. 1. Phases of Intrusion Detection System.

Intrusion detection system consists of four main parts as data collection, feature selection, analysis and action as shown in Fig. 1.

- **Data Collection :** The dataset is given as input to ID System.
- **Feature Selection :** Various features as duration, protocol_type, service, src bytes, dst_bytes all are extracted, processed and given to the second stage.
- **Analysis :** The data is analysed for its correctness.
- **Action :** It states the reaction of attack over the system.

4.1 Deep Neural network (DNN)

A deep neural network (DNN) is an artificial neural network (ANN) with numerous layers between the input and output layers. DNN helps in finding the correct mathematical calculations to convert the input into the output, as input may be a linear or a non-linear relationship.

Working Connections between neurons are associated with a weight, dictating the importance of the input value. All 42 attributes will be given as input to the first layer of DNN then on the second layer for each hidden unit, we will compute its value based on previous layer output and so on. Neurons apply an Activation Function on the data to "standardize" the output coming out of the neuron. each attribute in dataset has it's own importance in finding whether this will lead to attack or not so in training phase deep neural model is trained in such a way that if any data packet comes with its out of threshold value then it will be classified as attack otherwise not an attack, weights of neuron will be adjusted with consideration of bias and activation function. Value of any neuron is shown by f(x).

$$\mathrm{f(x)} = \mathrm{W_1X_1} + \mathrm{W_2X_2} + \mathrm{W_3X_3} + \ldots + \mathrm{W_{42}X_42} + \mathrm{B} \tag{1}$$

Where W_n= Weight of each unit, X_n= attribute and B is the Bias.

4.2 Artificial Neural Network (ANN)

ANN or neural networks are computational algorithms. It is intended to mimic the behavior of biological systems composed of the "neurons". ANN is initialized with a classifier as Sequential. There is one input layer, 3 hidden layers and output layer where "relu" is used as an activation function for the input and hidden layer and "sigmoid" for the output layer. The ANN compiled using an optimizer used as "adam". The model is trained and a confusion matrix is observed and various performance metrics are calculated.

Working The arrow between the two layers represents connectivity joining the two neurons. It is used to signify the channel for the flow of data. It was observed that each relation has a load, an integer number that is owned to rule the signal connecting the two neurons. If the output is fine that was produced by the network then we don't need to adjust the loads. Also if the bad output is produced, then firmly the system will modify the loads to upgrade the results.

4.3 Naive Bayes

It is a classification method based on the popular Bayes theorem with an assumption of independence among predictors. Here the classifier is used as GaussianNB, i.e. fitting Naive Bayes to the Training set. After that, the test set results are predicted and a confusion matrix is observed.

Working Naive Bayes is Bayes theorem based algorithm in which it will classify into four category based on probability $P(A/B) = [P(B/A).P(A)]/P(B)$, where $P(A/B)$ finds what is the probability of being classified into one of the attack category given all 42 attributes. Eg. Let any packet that enters the system through a LAN port, we will extract all info about the packet (length, checksum, header length, etc). In the naive Bayes algorithm, all of these 42 attributes will be treated as prior to determining posterior info (classification).

4.4 Logistic Regression

Logistic Regression is a Machine Learning algorithm which is used for classification problems, it is a predictive analysis algorithm, and based on the concept of probability. The classifier is used as Logistic Regression. The confusion matrix is observed and various performance metrics are calculated.

Working This is a simple algorithm in which we will find y(output) based on multiple input variables (all 42 attributes).

$$\mathrm{y} = \mathrm{M}_0 + \mathrm{M}_1\mathrm{A}_1 + \mathrm{M}_2\mathrm{A}_2 + \mathrm{M}_3\mathrm{A}_3 + \ldots + \mathrm{B} \tag{2}$$

Where M is coefficient for various attributes and B is the Bias, A_n are the attributes that are multiple variables. It will give the best fit line among the dataset data samples will be divided by line, distance between the data point and line is considered as error.it uses maximum liklihood function to find the best fit line among the datapoints in dataset.

4.5 Decision Tree

Decision Tree is a non-invariable supervised learning algorithm that is owned for both classification as well as regression of the tasks. The aim is to build a model that forecast the value of a target variable by gaining simple decision based rules deduced from the data quality. The classifier is used as a DecisionTreeClassifier. The confusion matrix is observed and various performance metrics are calculated.

Working Decision Tree will take input at the root of all the data points, on each node partial decision of being classified into one of four categories will be determined and leaf node will work as a final destination where four nodes will represent that. For each row in training dataset prediction will be there, and we will check whether our model classified correctly or not based on the testing dataset.

4.6 Random Forest

Random Forest algorithm builds decision trees based on data trials and then forecasts from each of them and ultimately selects the finest solution by state of voting. The classifier is used as a RandomForestClassifier. The confusion matrix is observed and various performance metrics are calculated.

Working Firstly, random data samples are opted from a KDD training dataset. Next, this algorithm will build a decision tree for each and every sample. Then it will acquire the forecasted result from every decision tree that where it has to be classified in the attack category. Final voting says the overall attack pattern from all given sample dataset. At last, opt the most voted forecasted result as the ending prediction result as mentioned earlier.

Algorithm :
1. Load the dataset.
2. Apply pre-processing technique with Normalizer.
2.1 Normalize samples individually to unit norm.
3. Make a partition of train and test data.
4. Dataset is given input to Random Forest.
5. The test dataset is then provided to random forest for classification.
6. Calculate accuracy, Recall, Precision, F-measure and entropy.

5 Experiment and Results

All the model with their performance metrics is shown in Table 2. Among all the models Random Forest gives better accuracy, precision, f-measure, and least entropy as compared to others and Decision Tree shows best over recall in comparison to other models.

Table 2. Performance metrics for all algorithms.

Algorithms	**Accuracy**	**Recall**	**Precision**	**F-measure**	**Entropy**
DNN (1 layer)	0.99937	0.99792	0.99894	0.99843	0.00105
DNN (5 layer)	0.99908	0.99863	0.99673	0.99768	0.00326
Artificial Neural Network	0.99931	0.99877	0.99775	0.99826	0.00224
Naive Bayes	0.94803	0.79267	0.99911	0.88400	0.00088
Logistic Regression	0.99862	0.99602	0.99703	0.99652	0.00295
Decision Tree	0.99975	**0.99942**	0.99931	0.99937	0.00068
Random Forest	**0.99985**	0.99938	**0.99986**	**0.99962**	**0.00013**

So, we can observe that among all the algorithms, random forest shows the best accuracy, precision, and F-measure. The randomness measured by random forest is least among all. In case of recall, decision tree gives better results. So, overall we can say that decision tree algorithm has performed well over other algorithms.

We also compared our work to the existing papers as described in Table 3. Yuyang Zhou [12] proposed a heuristic algorithm called Correlation-based-Feature-Selection-Bat-Algorithm (CFS-BA) and concluded results over various datasets such as KDD CUP 99, NSL-KDD and CIC-IDS2017. By their method

Table 3. Results compared with existing work.

Authors	**Performance Metrics (KDD CUP 99)**
Yuyang Zhou [12]	0.976 (Accuracy) 0.998 (Precision) 0.998 (F-measure)
Proposed Work	
Random Forest	0.99985 (Accuracy), 0.99986 (Precision), 0.99962 (F-measure)

they achieved an accuracy of 0.976, precision of 0.998 as well as F-measure of 0.998 using KDD CUP 99 dataset, whereas in our work, we got an accuracy of 0.99985, precision of 0.99986 and F-measure of 0.99962 using KDD CUP 99 dataset. As well for the other dataset for the existing work, our accuracy for detecting the network intrusion is much better.

6 Conclusion and Future Work

IDS are fetching the head role for many institutions after establishing the firewall technology across the network circumference. IDS can supply protection from outside users and inner attackers, where traffic doesn't go behind the firewall. All the following points are should always be kept in mind. In the future, we will see a various algorithm that can give better results and also we will make one add-on which will be added to the browser.
Our proposed model works only on host side, this can further be extended to server side as well, KDD-cup 99 dataset is used for all proposed algorithms but newer version of dataset can be used with new deep learning model as well. Since latest version of KDD dataset contains more features it will give more accuracy over old dataset.

References

1. http://kdd.ics.uci.edu/databases/kddcup99/kddcup.data_10_percent.gz
2. Ansam Khraisat, Iqbal Gondal, Peter Vamplew Joarder Kamruzzaman.: Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecurity 2019.
3. Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan.: INTRUSION DETECTION SYSTEM, International Journal of Technical Research and Applications 5(2):2320-8163, April 2017.
4. Dr. S.Vijayarani and Ms. Maria Sylviaa.S.: INTRUSION DETECTION SYSTEM – A STUDY, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.
5. Rachna Kulhare, Divakar Singh.: Survey paper on intrusion detection techniques, INTERNATIONAL JOURNAL OF COMPUTERS TECHNOLOGY, 2013.
6. Bane Raman Raghunath, Shivsharan Nitin Mahadeo.: Network Intrusion Detection System (NIDS), First International Conference on Emerging Trends in Engineering and Technology, 2008.

7. Kinam Park, Youngrok Song, Yun-Gyung Cheong.: Classification of Attack Types for Intrusion Detection Systems using a Machine Learning Algorithm, Fourth International Conference on Big Data Computing Service and Applications, 2018.
8. Aditya Nur Cahyo, Risanuri Hidayat, Dani Adhipta.: Performance comparison of intrusion detection system based anomaly detection using artificial neural network and support vector machine, AIP Conference Proceedings 1755, 070011 (2016).
9. Amudha Arul, Karthik Subburathinam, S. Sivakumari .: Classification Techniques for Intrusion Detection An Overview, International Journal of Computer Applications 76(16):33-40, August 2013.
10. Rajesh Wankhede, Vikrant Chole.: Intrusion Detection System using Classification Technique, International Journal of Computer Applications (0975 – 8887), Volume 139 – No.11, April 2016.
11. Rashmi Ravindra Chaudhari, Sonal Pramod Patil.: INTRUSION DETECTION SYSTEM: CLASSIFICATION, TECHNIQUES AND DATASETS TO IMPLEMENT, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 02, Feb -2017.
12. Yuyang Zhou, Guang Cheng, Senior Member, IEEE, Shanqing Jiang, and Mian Dai.: An Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier, JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015.