# 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 maheshl5kankar@gmail.com
bhawanarudra@nitk.edu.in

**Abstract.** Intrusion Detection System (IDS) defined as a software application which we can trace the network or system activities and find if any malicious activity occurs. Outstanding growth and usage of the internet raises concerns about how to communicate and protect the digital information safely. In today's scenario attackers use different types of attacks for fetching the private information. Many of the Intrusion Detection techniques, methods and algorithms help to find those several attacks. The fundamental purpose of this project is to provide an overall study about the intrusion detection mechanism, types of intrusion detection methods, types of attacks, different tools and techniques, research needs and challenges.

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

## 1 Introduction

Intrusion Detection Systems (IDSs) are a range of cybersecurity based technology initially developed to find the vulnerabilities and exploits against a destination host. The sole use of the IDS is to detect threats. Algorithms of machine learning have played an essential part in the field of cyber security. The basic way is to use machine learning algorithms to build a model of trustworthy and fruitful activity, and then compare new behavior against this model.
We evaluated our project based on various performance metrics such as accuracy, recall, precision, f-measure and entropy. Accuracy is the ratio of number of correct predictions to the total number of input samples, precision (also called positive predictive value) is the fraction of necessary instances among the retrieved instances, while recall (also known sensitivity of data) is the part of the total amount of necessary instances that were actually retrieved. The F-measure (F1 score or F score) is a measurement 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, Bot-IoT 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 Anomaly based detection system and signature based intrusion detection. They also discussed about 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.

## 3 Methodology

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

- **Denial-of-Service-Attack (DoS) :**
- **User-to-Root-Attack (U2R) :** unauthorized access from a remote machine.
- **Remote-to-Local-Attack (R2L) :** unauthorized access to local superuser (root) privileges.
- **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 42th 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 the 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,<br>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.

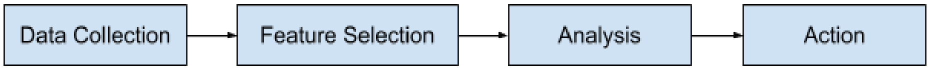

**Fig. 1.** Phases of Intrusion Detection System.

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 multiple layers between the input and output layers. The DNN finds the correct mathematical manipulation to turn the input into the output, whether it be a linear relationship 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. Value of any neuron is shown by f(x).

$$\mathrm{f(x)} = \mathrm{W_1X_1} + \mathrm{W_2X_2} + \mathrm{W_3X_3} + \ldots + \mathrm{W_{42}X_{4}2} + \mathrm{B} \tag{1}$$

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

### 4.2 Artificial Neural Network (ANN)

Artificial Neural networks 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 layer and output layer where "relu" is used as 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 a connection between two neurons. Also, they used to indicate the pathway for the flow of information. As it was noticed that each connection has a weight, an integer number that is used to control the signal between the two neurons. If the output is good that was generated by the network then we don't require to adjust the weights. Although, if poor output is generated, then surely the system will alter the weight to improve 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 determine 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 LogisticRegression. 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.

### 4.5 Decision Tree

Decision Tree is a non-parametric supervised learning algorithm that is used for both classification and regression of the tasks. The goal is to build a model that predicts the value of a target variable by learning simple decision based rules inferred from the data features. 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 root to 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 final destination where four nodes will represent that. For each row in training dataset prediction will be there, and for we will check whether our model classified correctly or not based on testing dataset.

### 4.6 Random Forest

Random Forest ML algorithm creates decision trees based on data samples and then predicts from each of them and finally selects the best solution by means of voting. The classifier is used as a RandomForestClassifier. The confusion matrix is observed and various performance metrics are calculated.

**Working** First, start with the selection of random samples from a KDD training dataset. Next, this algorithm will construct a decision tree for every sample (each row data). Then it will get the prediction 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, select the most voted prediction result as the final prediction result as mentioned earlier.

## 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** |

## 6 Conclusion and Future Work

IDS are becoming the main part for many organizations after deploying firewall technology at the network perimeter. IDS can provide protection from external users and internal attackers, where traffic doesn't go past the firewall at all. However, the following points are must to always keep in mind. If all of these points are not attached to, an IDS implementation along with a firewall alone cannot make a highly secured infrastructure. In future we will see various algorithm that can give better results and also we will make one add-on which will be added to the browser.

## 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. Bane Raman Raghunath, Shivsharan Nitin Mahadeo.: Network Intrusion Detection System (NIDS), First International Conference on Emerging Trends in Engineering and Technology, 2008.
6. Mohssine El Ajjouri, Siham Benhadou, Hicham Medromi.: New collaborative intrusion detection architecture based on multi agent systems, 2015 International Conference on Wireless Networks and Mobile Communications (WINCOM), 2015 Pages: 1 - 6.
7. Agustinus Jacobus, Alicia A. E. Sinsuw.: Network packet data online processing for intrusion detection system, 2015 1st International Conference on Wireless and Telematics (ICWT), 2015, Pages: 1 - 4.
8. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez .: Anomaly-based network intrusion detection: Techniques, systems and challenges, Computer Security, vol. 28., 2009
9. Bhavin Shah, Bhushan H. Trivedi .: Improving Performance of Mobile Agent Based Intrusion Detection System, 2015 Fifth International Conference on Advanced Computing  Communication Technologies, 2015, Pages: 425 - 430.
10. M. Dass, J. Cannady, W. D. Potter.: A blackboard-based learning intrusion detection system: a new approach, Developments in Applied Artificial Intelligence, Springer, 2003, pp. 385–390.