Journal for Research | Volume 08 | Issue 05 | July 2022
ISSN: 2395-7549

Behavioral Threat Analysis and Detection for Ids Using ATT&CK Matrix Framework

Sandhiya V
Department of Computer Science & Engineering
Sri Venkateswara Institute of Science and Technology, Tiruvallur, India

Abstract

Intrusion detection systems defines an important and dynamic research area for cyber security. The role of Intrusion Detection System within security architecture is to improve a security level by identification of all malicious and also suspicious events that could be observed in computer or network system. One of the more specific research areas related to intrusion detection is anomaly detection. The goal of this project is verification of the anomaly detection systems' ability using behavioural algorithms to resist the attack. The main focus of this is solved by using a deep network which passes information through several layers to learn the underlying hidden patterns of normal and attack network connection records and finally aggregates these learned features of each layer together to effectively distinguish the normal from the various attacks of network connection records. To achieve an acceptable detection rate, we tweak the various configurations of network settings and its parameters in deep network so that it is able to form behaviour based feature analysis to detect attacks like virus threats, man-in-the-middle attacks, Denial of Services and so on.

Keywords: Intrusion Detection System, Artificial Intelligence, Deep Neural Network, Modified NaiveBayes Intrusion Detection System, Anomaly detection

I. INTRODUCTION

The role of Intrusion Detection System within security architecture is to improve a security level by identification of all malicious and also suspicious events that could be observed in computer or network system. One of the more specific research areas related to intrusion detection is anomaly detection. Anomaly-based intrusion detection in networks refers to the problem of finding untypical events in the observed network traffic that do not conform to the expected normal patterns. It is assumed that everything that is untypical/anomalous could be dangerous and related to some security events. To detect anomalies many security systems implements a classification or clustering algorithms. However, recent research proved that machine learning models might misclassify adversarial events, e.g. observations which were created by applying intentionally non-random perturbations to the dataset. Such weakness could increase of false negative rate which implies undetected attacks. This fact can lead to one of the most dangerous vulnerabilities of intrusion detection systems. The goal of the research performed was verification of the anomaly detection systems ability to resist this type of attack. This project presents the preliminary results of tests taken to investigate existence of attack vector, which can use adversarial examples to conceal a real attack from being detected by intrusion detection systems. The aim of this Project is to study the use of an Intrusion Detection System in a network and try to use anomaly detection techniques to detect different types of attacks within the network. To study how a Network Intrusion Detection System that will detect abnormal network traffic in a network based on data such as header fields, logical addresses and secure port numbers. To present the test results of the Intrusion Detection System to ensure that it is performs the outlined intrusion detection and bandwidth management functions. To showcase the use of the intrusion detection system to protect information in an organization. When an intrusion-detection system is deployed, it becomes the natural primary target of hostile attacks, with the aim of disabling the detection feature and allowing an attacker to operate without being detected. Denial-of-service attacks, Distributed Denial-of-service attacks are a powerful and relatively easy way of temporarily disabling the intrusion-detection system. The attack can take place against the detector, by forcing it to process more information than it can handle (for example by saturating a network link). Evasion of the detection, several techniques have been developed to evade detection of an attack by intrusion-detection systems.

II. RELATED WORK

The protection of data against unauthorized access is the main objective of security. It can be guaranteed by security mechanisms. Researchers such as Vinayakumar R, Soman KP and Prabaharan Poornachandran [1] evaluates the effectiveness of various shallow and deep networks to NIDS in this paper. The shallow and deep networks are trained and evaluated on the KDDCup '99' and NSL-KDD data sets in both binary and multi-class classification settings. The deep networks are performed well in comparison to the shallow networks in most of the experiment configurations. The main reason to this might be a deep network passes information through several layers to learn the underlying hidden patterns of normal and attack network connection records and finally aggregates these learned features of each layer together to effectively distinguish the normal and various attacks of network

connection records. Additionally, deep networks have not only performed well in detecting and classifying the known attacks additionally in unknown attacks too. To achieve an acceptable detection rate, we used various configurations of network settings and its parameters in deep networks.

Works reported by Karuna S. Bhosale, Maria Nenova, [2] uses real time packet, which is used to real time analysis and also the KDD Cup 99 dataset for the execution. In this system they uses the different classifiers on this real time packets and KDD dataset for the comparison of obtained results and also we use the Data Pre-processing algorithm, Hybrid Feature Selection Algorithm and Modified Naive Bayes Algorithm. Using these algorithms we improve the system accuracy and execution performance. They uses LOIC DDoS assault generator instrument to make the assault at bundle getting time what's more use KDD compartment dataset for various assault pursue, for instance, DoS, R2L, L2R, Test.

Yousraberguig, Jalal laassiri, Sanaehanaoui [3] have tried several techniques of prevention, detection, tracing and identification to protect the system against DoS attacks. Among the powerful attacks that threaten the security of a system, we find Distributed Denial of Service attack. Recently, this type of attack has become an active research field. In fact, with the development of cloud computing and e-commerce applications, this threat is becoming more and more serious. The availability of several free online tools makes the attack an easy task for attackers which increase its rate. A Denial Of- Service (DoS) or Distributed Denial-Of-Service (DDoS) attack is defined as an attempt to make a machine or network resource unavailable to users. The general way to perform this type of attack is to flood the network by sending several requests to the server, to keep it busy for a long time and prevent legitimate users from getting the service. The goal is to suspend temporarily or indefinitely the services of a system and paralyzes it. The system can detect DOS attack by capturing the packets flowing in the network.

Parag Verma, Shayan Anwar, Shadab Khan and Dr. Sunil B Mane [4]. This paper proposes use of machine learning classification algorithms - XGBoost and AdaBoost with and without clustering to train a model for NIDS. The models are trained and tested using NSL KDD dataset and the results are an improvement over the previous works related to intrusion detection on the same dataset. Another approach to detect network intrusion is using Data mining based techniques. In this approach, the raw data points are clustered into different classes using feature selection, normalizing raw data and building fuzzy similar matrices. H. Han present an algorithm called Signature Apriori. This is capable of generating signatures for misuse detection IDS. The main feature of this method is that it not only uses attributes of transfer protocol, but alsothe content of traffic. Supervised learning based approaches can also give substantial results in intrusion detection scenarios. Bonifaciouse Multilayer perceptron Neural Networks to identify intrusive behaviour using Back propagation, Quick prop and Rprop as training algorithms. Mill and Inouepropose the TreeSVM and ArraySVM.

The paper presented by Samuel Hess, Pratik Satam, Gregory Ditzler and Salim Hariri [5] evaluates a specific application that is afflicted by these modern cyber security challenges: detection of malicious HTML files. Previous work presented a general framework for malicious HTML file classification that we modify in this work to use a c2 feature selection technique and synthetic minority oversampling technique (SMOTE). Unfortunately, collecting malicious HMTL files is extremely difficult and can be quite noisy from HTML files being mislabelled. We experiment with different classifiers (i.e., AdaBoost, Gentle-Boost, RobustBoost, RusBoost, and Random Forest) and a pure detection model (i.e., Isolation Forest). We benchmark the different classifiers using SMOTE on a real dataset that contains a limited number of malicious files (40) with respect to the normal files (7,263). It was found that the modified framework performed better than the previous framework's results.

Saqr Mohammed Almansob, Santosh ShivajiraoLomte [6] have proposed two approaches to addressing intrusion detection system problems. One of this approach is known as Principal Component Analysis (PCA) for feature extraction and applied Naive Bayes approach as a classification problem. So, the model applied on the KDD99 dataset. The obtained results show the increase in detection and accuracy rate as well as a decrease in false positive rate. The network exposed to attacks continuously which leading to stealing user's files and information. For this reason, must monitor and analysis all the traffic data on the network using intrusion detection system so false positive rate one of the intrusion detection problem which generates a lot of alert over network our challenge to reduce the false positive and improve the detection and accuracy rate in network. On other hand, intrusion detection system plays the role of mongering all the traffic data which grow through a network and analysis all the normal and malicious events over network. Furthermore, the attacks grew up and increased on the system which leads to the loss of a lot of important information.

III. PROPOSED METHODOLOGY

Intrusion Detection System (IDS) uses machine learning and deep learning techniques to detect anomalies in the network. The signature of the anomalies are trained through a deep learning neural network and the corresponding weights and biases are saved in a database.

The feature sets of each connection records are preprocessed and normalized. To classify the connection record as either normal or attack, we used various classical machine learning classifiers for KDDCup '99'. The performance of them is known by confusion matrix.The confusion matrix provides class-specific metrics such as overall accuracy, precision, recall, f-measure, true-positive-rate (TPR) and false positive- rate (FPR). Deep networks pass the connection records to more than one hidden layers. Each hidden layer has a non-linear function. As a result deep networks learns the non-linear or highly varying patterns in connection records of training dataset to distinguish them as normal or attack. Examines the effectiveness of shallow and deep networks to NIDS task by modeling the connection records of Transmission Control Protocol / Internet Protocol (TCP/IP) information. Deep networks

performed well in comparison to the shallow networks in distinguishing the connection records as either normal or an attack and additionally in categorizing an attack to corresponding attack categories too.

IV. ARCHITECTURE DIAGRAM

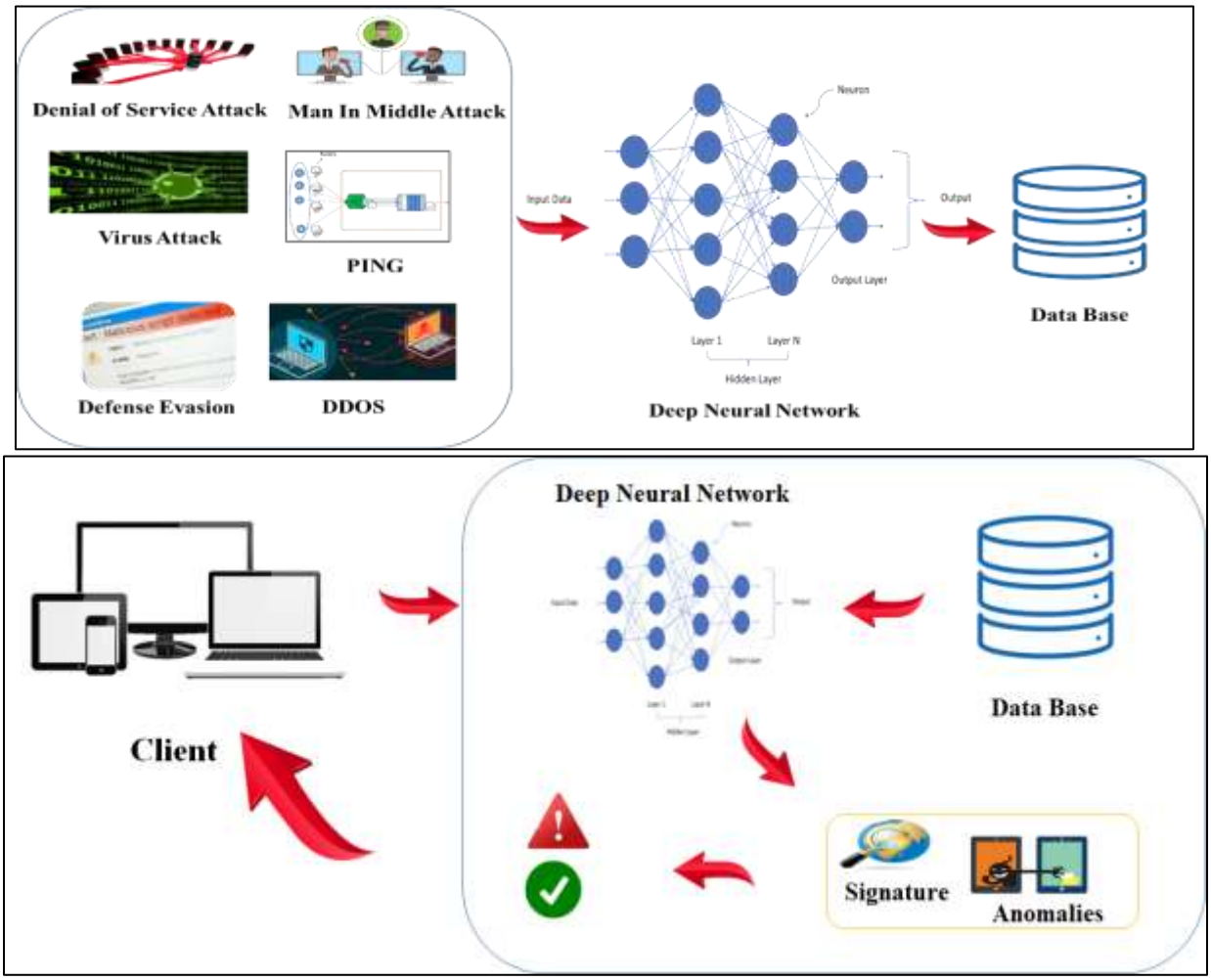

Fig. 1: Architecture of Intrusion Detection System

A network intrusion detection system (NIDS) monitors the packets that traverse a given network link. A Network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. Such a system operates by placing the network interface into promiscuous mode, affording it the advantage of being able to monitor an entire network while not divulging its existence to potential attackers. Because the packets that a NIDS is monitoring are not actually addressed to the host the NIDS resides on, the system is also impervious to an entire class of attacks such as the ping-of-death attack that can disable a host without ever triggering a HIDS. A NIDS is obviously of little value in detecting attacks that are launched on a host through an interface other than the network.

A network-based ID can monitor traffic only in its local network segment. In switched and routed networks, a sensor is required in each segment (collision domain) in which network traffic is to be monitored. When a sensor detects a possible intrusion, it will report it to a central management console, which will take care of the appropriate passive or active response. Communication between the remote sensor and the management console should be secure to avoid interception or alteration by the intruder. One major shortcoming of NIDS is that they are oblivious to local root attacks. The authorized user of the system that attempts to gain additional privileges will not be deleted if attack is performed locally. The authorized user of the system may be able to set up an encrypted channel when accessing the machine remotely.

The network card of a network-based IDS runs in promiscuous mode, which means it picks up all traffic from the media even if the destination address is not the IDS. It basically works like a sniffer.

On a heterogeneous network, a NIDS generally does not possess intimate knowledge of all of the hosts on the network and is incapable of determining how a host may interpret packets with ambiguous characteristics. Without explicit knowledge of a host system's protocol implementation, a NIDS is impotent in determining how a sequence of packets will affect that host if different implementations interpret the same sequence of packets in different ways. Protocol ambiguities can also present a

problem to a NIDS in the form of crud. Crud appears in a network stream from a variety of sources including erroneous network implementations, faulty network links, and network pathologies that have no connection to intrusion attempts. If a NIDS performs insufficient analysis on a stream containing crud, it can generate false positives by incorrectly identifying this crud as being intrusive. While a NIDS therefore is in a very convenient position whereby it has complete access to all packets traversing a network link, its perspicacity is challenged due to ambiguities in network data and its limited perspective of host system implementations and network topology. NIDS should be capable of standing against large amount number of network traffic to remain effective. As network traffic increases exponentially NIDS must grab all the traffic and analyse in a timely manner.

A. List of Modules

1) Packet Decoder
2) Pre-processors
3) Feature Selection
4) Detection System
   a) Signature Based Detection
   b) Anomaly Detection
5) Logging System

B. Module Description

1) Packet Decoder

The packet decoder collects packet from different-2 network interfaces and then send to be pre-processor or sent to the detection engine. Network interface might be Ethernet. Data packets are the basic entities of all communication systems. Security of a network thus implies security of the data packets. The enormous attacks from the internet increase day by day. The quality of service is became more issue hence it should require powerful traffic analysis and distribution engine for network application. The complete packet inspection is required to examine the data part along with the header content of the packet. A packet analyser is a computer software or hardware that can intercept and log traffic passing through a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyses its content according to the appropriate specification.

2) Preprocessors

It works to modify or arrange the packet before detection engine to apply some operation on packet if packet is corrupted. Sometimes they also generate alert if any anomalies found in the packet. Basically it matches the pattern of whole string so, by changing the sequence or by adding some extra value intruder can fool the IDS but pre-processor re-arranges the string and IDS can detect the string. Pre-processor does one very important task i.e. defragmentation. Because sometimes intruder break the signature into two parts and send them in two packets so, before checking the signature both packet should be defragmented and only then signature can be found and this is done by pre-processor. The Detection Engine Its main work is to find out intrusion activity exits in packet with the help of rules and if found then apply appropriate rule otherwise it drops the packet. It takes different time to respond different packet and also depends upon the power of machine and number of rules defines in the system.

3) Feature Selection

Feature selection is an effective and an essential step in successful high dimensionality data applications. It is often an essential data processing step prior to applying a learning algorithm. Reduction of the attribute space leads to a better understandable model and simplifies the usage of different visualization technique. There are two common approaches for feature reduction. A Wrapper uses the intended learning algorithm itself to evaluate the usefulness of features, while filter evaluates features according to heuristics based on general characteristics of the data. The wrapper approach is generally considered to produce better feature subsets but runs much more slowly than a filter.

4) Detection System

a) Signature Detection Or Misuse Detection

The concept behind signature detection or misuse detection scheme is that it stores the sequence of pattern, signature of attack or intrusion etc into the database. When an attacker tries to attack or when intrusion occurs then IDS matches the signatures of intrusion with the predefined signature that are already stored in database. On successful match the system generates alarm. In misuse detection, the IDS analyses the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. Like a virus detection system, detection software is only as good as the database of intrusion signatures that it uses to compare packets against.

The essence of misuse detection centres around using an expert system to identify intrusions based on a predetermined knowledge base. As a result, misuse systems are capable of attaining high levels of accuracy in identifying even very subtle intrusions that are represented in their expert knowledge base; similarly, if this expert knowledge base is crafted carefully, misuse systems produce a minimal number of false positives. A less fortunate ramification of this architecture results from the fact that a misuse detection system is incapable of detecting intrusions that are not represented in its knowledge base. Subtle variations of known attacks may also evade analysis if a misuse system is not properly constructed. Therefore, the efficacy of the system relies heavily on the thorough and correct construction of this knowledge base, a task that traditionally requires human domain experts.

The unknown attacks cannot be detected using signature-based IDS. Since the detecting unknown attacks, IDS is applied yet, this method cannot completely distinguish between sophisticated attacks and known attack. This represents a method achieve unknown attacks that in the archive have not been stored. This method is poor in second stage classifier to a detection rate of unknown attacks.

The signature fragments were extracted and converted into the standard rules of the intrusion detection systems for subsequence defence.

b) Anomaly Detection

Anomaly detection is concerned with identifying events that appear to be anomalous with respect to normal system behaviour. The most appealing feature of anomaly detection systems is their ability to identify new and previously unseen attacks. Each of these anomaly-based approaches fundamentally relies upon the same principles: anomalous activity is indicative of an attempted attack and the correct set of characteristics can sufficiently differentiate anomalies from normal system usage.

In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies. Such system involves first establishing a baseline model that represents normal system behaviour and against which anomalous events can be distinguished. The system then analyses an event by considering it within this model and classifying it as anomalous or normal based on whether it falls within a certain threshold of the range of normal behaviour. Because the process of establishing a baseline model of normal behaviour is usually automated, anomaly systems also do not require expert knowledge of computer attacks. This approach is not without its handicaps; however, as anomaly detection may fail to detect even attacks that are very well-known and understood if these attacks do not differ significantly from what the system establishes to be normal behaviour. Anomaly based systems are also prone to higher numbers of false positives, as all anomalous events are assumed to be intrusive although in reality a variety of other factors can produce behaviour that appears anomalous.

5) Logging System

Whatever detection engine finds in the packet, it might generate an alert or used to log activity. All log files are kept by default location can be changed. For logging in binary format, don't need all options. The binary format makes packet collection much faster, because it doesn't have to translate the data into human readable format.

C. *Sequence Diagram*

Sequence diagrams are best suited to the portrayal of simple interactions among relatively small numbers of objects. As the number of objects and messages grows, a collaboration diagram can become difficult to read. Several vendors offer software for creating and editing sequence diagrams.

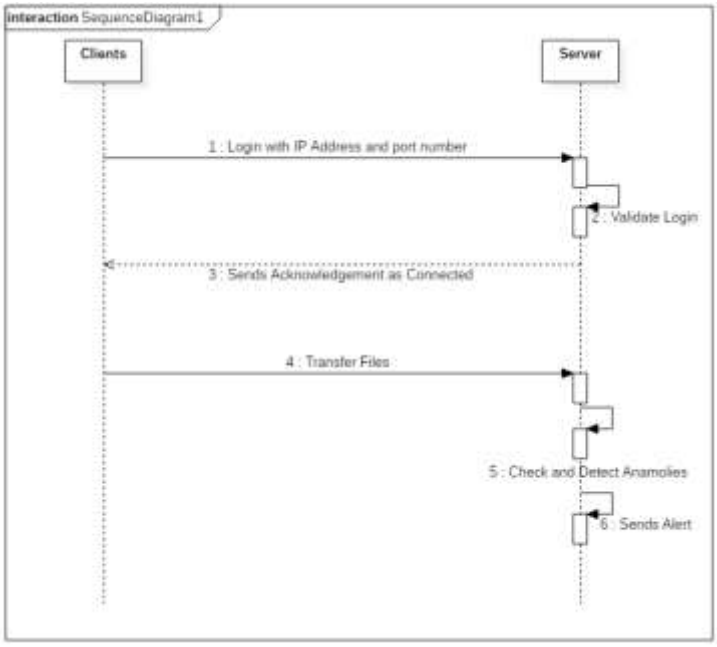

Fig. 2: Sequence Diagram of Intrusion Detection System

V. RESULT & DISCUSSION

The previous method has proposed an approach to develop efficient IDS by using the principal component analysis (PCA) and the random forest classification algorithm. Where the PCA will help to organize the dataset by reducing the dimensionality of the dataset and the random forest will help in classification. Results obtained states that the previous approach works more efficiently

in terms of accuracy as compared to other techniques like SVM, Naïve Bayes, and Decision Tree. This system can collect a large number of alerts in a day, overloading your work. FP alerts can also be very high, which leads to less confidence on alerts. If you try to cut down False Positive rate, then this can affect NIDS reliability. Tasks like analysing and filtering has to be done manually. Signature based IDS are unable to detect novel attacks, suffer from false alarms, and have to program again for every new pattern to be detected. To Host based IDS, kind of information needed to be logged, Unselective logging of messages may greatly increase the audit and analysis burden. Selective logging runs the risk that attack manifestations could be missed. The results obtained by proposed method are having the values for performance time (min) is 3.24 minutes, Accuracy rate (%) is 96.78 %, and the Error rate (%) is 0.21 %. To improve an acceptable detection rate, we provided the various configurations of network settings and its parameters in deep network so that it is able to form a behavior based feature analysis to detect various attacks. We demonstrate the likely overtraining by determining that a subset of the malicious files, while suspicious, did not come from a malicious source.

A. Performance Metrics in IDS

There are many classification metrics for IDS, some of which are known by multiple names. Below image shows the confusion matrix for a two-class classifier which can be used for evaluating the performance of an IDS. Each column of the matrix represents the instances in a predicted class, while each row represents the instances in an actual class.

B. Confusion Matrix

A Confusion matrix is the comparison summary of the predicted results and the actual results in any classification problem use case. The comparison summary is extremely necessary to determine the performance of the model after it is trained with some training data.

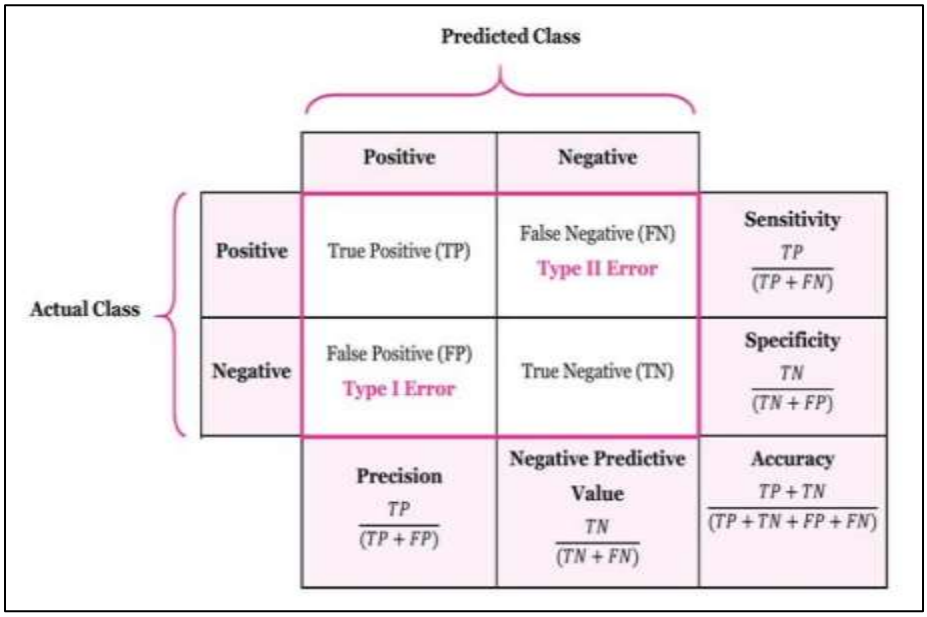

Fig. 3: Confusion matrix

Actual Class 1 value= 1 which is similar to Positive value in a binary outcome.
Actual Class 2 value = 0 which is similar to a negative value in binary outcome.
There are various components that exist when we create a confusion matrix. The components are mentioned below

- Positive(P): The predicted result is Positive (Example: Image is a cat)
- Negative(N): the predicted result is Negative (Example: Images is not a cat)

True Positive(TP): Here TP basically indicates the predicted and the actual values is 1(True)
True Negative(TN): Here TN indicates the predicted and the actual value is 0(False)
False Negative(FN): Here FN indicates the predicted value is 0(Negative) and Actual value is 1. Here both values do not match. Hence it is False Negative.
False Positive(FP): Here FP indicates the predicted value is 1(Positive) and the actual value is 0. Here again both values mismatches. Hence it is False Positive.

C. Performance metrics for IDS:

IDS are typically evaluated based on the following standard performance measures:

True Positive Rate (TPR): It is calculated as the ratio between the number of correctly predicted attacks and the total number of attacks. If all intrusions are detected then the TPR is 1 which is extremely rare for an IDS. TPR is also called a Detection Rate (DR) or the Sensitivity. The TPR can be expressed mathematically as

TPR = TP/ (TP+ FN)

False Positive Rate (FPR): It is calculated as the ratio between the number of normal instances incorrectly classified as an attack and the total number of normal instances.

$$FPR = FP/(FP + TN)$$

False Negative Rate (FNR): False negative means when a detector fails to identify an anomaly and classifies it as normal. The FNR can be expressed mathematically as:

$$FNR = FN /(FN + TP)$$

Classification rate (CR) or Accuracy: The CR measures how accurate the IDS is in detecting normal or anomalous traffic behavior. It is described as the percentage of all those correctly predicted instances to all instances:

$$Accuracy =(TP + TN)/(TP+ TN + FP + FN)$$

Receiver Operating Characteristic (ROC) curve: ROC has FPR on the x-axis and TPR on the y-axis. In ROC curve the TPR is plotted as a function of the FPR for different cut-off points. Each point on the ROC curve represents a FPR and TPR pair corresponding to a certain decision threshold. As the threshold for classification is varied, a different point on the ROC is selected with different False Alarm Rate (FAR) and different TPR. A test with perfect discrimination (no overlap in the two distributions) has a ROC curve that passes through the upper left corner (100% sensitivity, 100% specificity).

Confusion matrix:

[[19 4]
[2 70]]

Outcome values:

19 4 2 70

Table – 1
Classification report:

	precision	***recall***	***f1-score***	***support***
1	***0.90***	***0.83***	***0.86***	***23***
0	***0.95***	***0.97***	***0.96***	***72***
Accuracy			***0.94***	***95***
Macro avg	***0.93***	***0.90***	***0.91***	***95***
Weighted avg	***0.94***	***0.94***	***0.94***	***95***

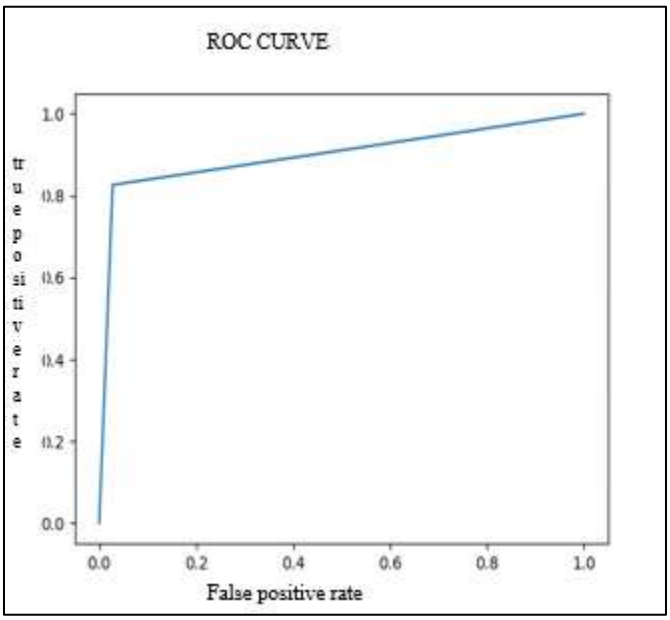

Fig. 4: Receiver Operating Characteristic

Figure reflects how accurate the prediction is: the area under the curve is what reflects the accuracy in prediction. A higher area under the curve is desired.

Intrusion detection system can be a physical appliance or security software to monitor the network traffic in order to detect suspicious activity. Many IDS keep information about the detected intrusions in a log file for further analysis or to combine these logs with other data to make policy and decisions. Network security is a large and growing area of concern for every network. The more we invent for the good of humanity, humans try to negate the good factor and hence the fear of viruses and hacking. Research has to move in the direction of preserving and guarding network environments which today are facing an ever increasing number of security threats in the form of Trojan worm attacks and viruses that can damage the Computer systems and communication channel. Firewalls are used as a security check point in a network environment; nevertheless there are still various types of security issues which are on the rise. In order to strengthen the network from illegal access the concept of IDS (Intrusion Detection System) is gaining popularity around the world. The applications of the data in the computer security field improves the

development of IDS in order to work on these applications it is essential to classify the degree of attacks in IDS and use it through data.

VI. CONCLUSION

Network threats are a security risk which can be met on a daily basis. Because of this, it is important today to consider more complex security options than just ordinary firewall systems. This project deals about various types of attack on networks, various classification of IDS and used approaches for IDS. This project finds out the problem associated with secure communication over the networks. The focus is to build a strong classification model for use in IDS. A strong classification model means one which can give near-perfect results. This will lead to a stronger IDS, the IDS when deployed in a certain network will make it more secure, and there will be much fewer chances of intrusion as the classification model running is of very high standard. The next bit is using the IDS as a sensor to alert the administrator about any irregularities. The IDS can be used as a one- stop device to extract information about the network. So, IDS can also act as a data source and its machine learning capabilities make it a flexible technology, avoiding regular updating. The IDS in future can also be made interactive with IoT devices. It can also form an integral part of Artificial Intelligence, as security is also a problem in the robotic world (even robots can be hacked). The airplanes, cars, mobile networks, the world of IoT, Artificial Intelligence, smart devices, all need IDS sensors employed in their architecture. Basically, anything that has internet and machines involved can use IDS as a security feature. The future world needs its privacy intact, so the developing robotic technology that will do a lot of work in future needs IDS. There is nothing perfectly safe in a network and there must be an IDS in a network to monitor everything, as people travelling in planes, cars, etc. should be able to trust the machines that are responsible for dropping them home. For example, any hacking resulting in a plane getting hijacked due to intrusions in the network can lead to devastating results. The focus is to build a strong classification model for use in IDS. A strong classification model means one which can give near-perfect results. This will lead to a stronger IDS, the IDS when deployed in a certain network will make it more secure, and there will be much fewer chances of intrusion as the classification model running is of very high standard. The next bit is using the IDS as a sensor to alert the administrator about any irregularities. This proposed algorithm gives a higher accuracy, it offers flexibility and can accept diverse data as inputs and finally has been deployed in industries to tackle large number of data.

REFERENCES

[1] Evaluating effectiveness of shallow and deep networks to intrusion detection system, Vinayakumar R, Soman Kp And Prabaharan poornachandran, IEEE 2017.
[2] Modified Naive Bayes Intrusion Detection System, Karuna S. Bhosale Maria Nenova, IEEE 2018.
[3] Dos Detection based on mobile agent and Naive Bayes Filter, Yousra Berguig, Jalal Laassiri, Sanae Hanaoui, IEEE 2018.
[4] Network Intrusion Detection using clustering and gradient boosting, Parag Verma, Shayan Anwar, Shadab Khan And Dr. Sunil B Mane, IEEE 2018.
[5] Malicious HTML file prediction: a detection and classification perspective with noisy data, Samuel Hess, Pratik Satam, Gregory Ditzler And Salim Hariri, IEEE 2018.
[6] Addressing challenges for Intrusion Detection System using Naive Bayes And PCA Algorithm, Saqr Mohammed Almansob, Santosh Shivajiraolomte, IEEE 2017.
[7] An analysis of recurrent neural networks For Botnet Detection Behaviour ,P.Torres, C. Catania, S. Garcia, And C. G. Garino, IEEE, 2016.
[8] Techniques to detect dos and DDOS attacks and an introduction of a mobile agent system to enhance it in cloud computing, A. Saidi, E. Bendriss, IEEE 2017.
[9] Flooding attacks detection of mobile agents in IP networks, J. Tajer, M. Adda, B. Aziz, IEEE 2017.
[10] Distributed Intrusion Detection using mobile agents in wireless body area networks, A. Odesile, G. Thamilarasu, Seventh, IEEE 2017.